UNIVERSITY OF VAASA

FACULTY OF TECHNOLOGY

TELECOMMUNICATIONS ENGINEERING

Mehmet Serif TAS

WI-FI ALLIANCE HOTSPOT 2.0 SPECIFICATION BASED NETWORK DISCOVERY, SELECTION, AUTHENTICATION, DEPLOYMENT AND FUNCTIONALITY TESTS.

Master´s thesis for the degree of Master of Science in Technology submitted for inspection in Vaasa, 25th of October, 2013.

Supervisor	Prof. Timo Mantare
Instructor	M.Sc .(Tech) Reino Lähdemäki Johan Kaustinen (Anvia Oyj)

ACKNOWLEDGMENTS

In the name of Allah S.W.T., the most Beneficent, the most Merciful thus this thesis has been possible.

I would like to express the deepest appreciation to my supervisor Professor Timo Mantere, who has given a great support and untiring guidance during this thesis work. I would like to express the deepest appreciation to my Professor Mohammed Salem Elmusrati, who has gained me a lot during his valuable lectures. I would also like to express the deepest gratitude to my instructors Reino Lähdemäki and Johan Kaustinen, who have provided me such a great opportunity to do my master's thesis for ANVIA. Their valuable questions and our discussions during our regular meetings, interest in this thesis work, support for the testing phase and most importantly their encouraging attitude have made this dream come true. Without their supervision and constant help this master's thesis would not have been possible.

My sincere thanks go to Jukka Rajaheimo, Hannes Kinnari, Karri Huhtanen and Jake-Matti Lahtinen for their support and contribution during the thesis work.

My sincere thanks also go to Professor Mohammed Salem Elmusrati, Tobias Glocker, Ruifeng Duan and Mulugeta Fikadu. I must indicate that I have gained a lot by attending their lectures.

This thesis work has been founded by ANVIA Oyj. First of all, it was a great experience for me to work in a very friendly environment and it was a great opportunity to take part in such a project based on WFA Hotspot 2.0 Specification that is predicted to be used by millions in near future. Moreover, I am really honored to be the first person testing/using this technology in Finland.

I would like to thank my family for supporting me financially and spiritually throughout my life and also I would like to thank my friends that always stand beside me and inspire me with their encouraging words.

TABLE OF CONTENT

LIST OF ABBREVIATIONS

3GPP	3rd Generation Partnership Project
AAA	Authentication, Authorization, And Accounting
ADDTS	Additional Step Required For Access
AES	Advanced Encryption Standard
AIH	Alert Identifier Has
ANDSF	Access Network Discovery And Selection Function
ANQP	Access Network Query Protocol
ANT	Access Network Type
AP	Access Point
ARP	Address Resolution Protocol
ASRA	Additional Step Required For Access
BSSID	Basic Service Set Identifier
BW	Bandwidth
CCK	Complementary Code Keying
CCMP	Counter Cipher Mode With Block Chaining Message Authentication Code Protocol
CHAP	Challenge-Handshake Authentication Protocol
CM	Connection Manager
CPE	Customer-Premises Equipment
CRL	Certificate Revocation List
CSMA/CA	Carrier Sense Multiple Access With Collision Avoidance
CTS	Clear To Send
DB	Data Base
DHCP	Dynamic Host Configuration Protocol
DLS	Direct Link Setup
DNS	Domain Name Server
DoS	Denial Of Service
DSCP	Differentiated Services Code Point
DSSS	Direct Sequence Spread Spectrum

EAP	Extensible Authentication Protocol
EAPoL	EAP Over LAN
EAP-AKA	EAP- Authentication And Key Agreement
EAP-GTC	EAP- Generic Token Card
EAP-MD5	EAP- Message Digest 5
EAP-SIM	EAP- Subscriber Identity Module
EAP-TLS	EAP- Transport Layer Security
EAP-TTLS	EAP-Tunneled Transport Layer Security
EAS	Emergency Alert System
EDXL	Emergency Data Exchange Language
ESR	Emergency Services Reachable
FAQ	Frequently Asked Questions
FCS	Frame Check Sequence
FQDN	Fully Qualified Domain Name
FTP	File Transfer Protocol
GAS	Generic Advertisement Service
GHz	Giga Hertz
GRE	Generic Routing Encapsulation
GSM	Global System For Mobile Communications
GTK	Group Transient Key
HESSID	Homogenous Extended Service Set Identifier
HLR	Home Location Register
HMAC-SHA1	Keyed-Hash Message Authentication Code
HO	Hotspot Operator
HTTP	Hypertext Transfer Protocol
ICMP	Internet Control Message Protocol
ID	Identity
IEEE	Institute Of Electrical And Electronics Engineers
IETF	Internet Engineering Task Force
IP	Internet Protocol
IPsec	Internet Protocol Security

IPTV	Internet Protocol Television
IPv4	Internet Protocol Version 4
IR	Infrared
ITU	International Telecommunication Union
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
LMD	Load Measurement Duration
MAC	Medium Access Control
MAN	Metropolitan Area Network
MAP	Mobile Application Part
Mbps	Megabit Per Second
MCC	Mobile Country Code
MHz	Mega Hertz
MIF	IETF Multiple Interfaces Working Group
MIH	Media-Independent Handover
MIMO	Multiple Input, Multiple Output
MK	Master Key
MLPP	Multiple Level Precedence And Preemption
MMPDU	Multi-Level Precedence And Preemption
MNC	Mobile Network Code
MSDUs	MAC Service Data Unit
MS-CHAP	Microsoft Version Of The Challenge-Handshake Authentication Protocol
MS-CHAPv2	Microsoft Version Of The Challenge-Handshake Authentication Protocol Version 2
NAI	Network Access Identifier
NAPT	Network Address And Port Translation
NAS	Network Access Server
NGH	Next Generation Hotspot
OASIS EDXL	OASIS Emergency Data Exchange Language
OFDM	Orthogonal Frequency Division Multiplexing

OI	Organization Identifier
OMA	Open Mobile Alliance
OMA-CMAPI	OMA-Connection Management Access Point Interface
P2P	Peer To Peer
PAME-BI QAM	Pre-Association Message Exchange BSSID Independent
PAP	Password Authentication Protocol
PDA	Personal Digital Assistant
PEAP	Protected Extensible Authentication Protocol
PIN	Personal Identification Number
PLMN	Public Land Mobile Network
PMK	Pairwise Master Key
PSK	Phase Shift Keying
PTK	Pair-Wise Transient Key
QAM	Quadrature Amplitude Modulation
QoS	Quality Of Service
QRLL	Query Response Length Limit
RADIUS	Remote Authentication Dial In User Service
RAN	Radio Access Network
RC4	Ron's Code 4, Rivest Cipher 4
RF	Radio Frequency
RTS	Request To Send
SIM	Subscriber Identity Module
SP	Service Provider
SQL	Structured Query Language
SSID	Service Set Identifier
SSP	Subscription Service Provider
SSPNs	Subscription Service Provider Network
STA	Station
TCP	Transmission Control Protocol
TDLS	Tunneled Direct Link Setup
TKIP	Temporal Key Integrity Protocol

TLS	Transport Layer Security
TSPEC	Traffic Specification
UDP	User Datagram Protocol
UE	User Equipment
UESA	Unauthenticated Emergency Service Accessible
UP	User Priority
URL	Uniform Resource Locator
USIM	UMTS Subscriber Identity Module
VPN	Virtual Private Network
WAN	Wireless Access Network
WBA	Wireless Broadband Alliance
WEP	Wired Equivalent Privacy
WFA	Wi-Fi Alliance
Wi-Fi	Wireless Fidelity
WLAN	Wireless Local Area Network
WLC	Wireless LAN Controller
WN	Wireless Network
WPA	Wi-Fi Protected Access
WPA2	Wi-Fi Protected Access 2

TABLE OF TABLES

TABLE OF FIGURES

UNIVERSITY OF VAASA
Faculty of technology
Author: Mehmet Serif Tas
Topic of the Thesis: Wi-Fi Alliance Hotspot 2.0 Specification Based Network Discovery, Selection, Authentication, Deployment And Functionality Tests.

Supervisor: Timo Mantere
Instructors: Reino Lähdemäki
Johan Kaustinen
Degree: Master of Science in Technology
Degree Programme: Department of computer science
Major of Subject: Degree Program in Telecommunications Engineering
Year of Entering the University: 2011
Year of Completing the Thesis: 2013 **Pages: 112**

ABSTRACT:

The demand for high mobile data transmission has been dramatically enlarged since there is a significant increase at the number of mobile communication devices that capable of providing high data rates. It is clearly observed that even the next generation cellular networks are not able to respond to this demand to provide the required level of mobile data transmission capacity. Although, WLAN responses to this demand by providing upwards of 600 Mbps data rates it is not convenient in terms of cellular like mobility and requires user intervention anytime of reconnection to a hotspot. Therefore, the need for a new technology took place and IEEE has introduced a new amendment to IEEE 802.11 standards family which is called as IEEE 802.11u. Based on IEEE 802.11u amendment, WFA developed WFA Hotspot 2.0 Specification and started to certify the Wi-Fi devices under Passpoint certification program. This new technology developed to provide Wi-Fi capable devices simply identify, select and associate to a Hotspot without any user intervention in a highly secure manner.

As Hotspot 2.0 Specification is quite new in the market it has been a challenging work to reach some academic papers; however, IEEE 802.11u standard, Internet sources, white papers published by different companies/organizations and discussions with telecommunication experts have made this master thesis to achieve its goals.

This thesis work provides a great resource for the network operators to have a great understanding of the Hotspot 2.0 Specification in terms of theory, network element requirements and deployment by providing a good understanding of the system functionality. In this paper, a comprehensive theoretical background that addresses to WLAN technology, Passpoint elements, and IEEE 802.11u based network discovery, selection and authentication is provided. Besides, Hotspot 2.0 network deployment scenarios with network core element requirements are designed and Passpoint functionality tests are performed under different scenarios by describing a comprehensive setup for the testing.

KEYWORDS: WFA Hotspot 2.0, IEEE 802.11u, ANQP, Passpoint, WLAN Security.

1. INTRODUCTION

High data traffic has overwhelmed cellular networks as there is a significant increase at the number of smartphones and it is expected that 800 million such devices additionally will get into the market in 2013 (Rukus 2013a). Subscribers switch to smartphones and tablets; as a result of this, mobile operators find them in a vast need to seek for technologies that can provide them high data transmissions to deal with all this traffic. While the expected technology is considered to provide off-loading for mobile operators, it has also been thought to provide a cellular based internet connectivity for non-SIM based mobile devices that do not rely on existing cellular networks such as GSM and 3G.

Globally, almost 70% of all smartphone-originated data flow is held via wireless fidelity (Wi-Fi) (Informa 2012). By having upwards of 600 Mbps data rate, Wi-Fi is considered to be an excellent choice as it supports dense access point (AP) utilizations, is available on all communication devices (smartphones, tablets etc.), and it is available to users in all common locations such as stadiums, arenas, airports, convention centers, colleges, train stations, downtown city center and so on (Rukus 2013a).

Wi-Fi alliance (WFA) realized the need to extend the capabilities of the former Wi-Fi networks to enhance the mobility experience to have a cellular-like implementation as Wi-Fi devices are being used with an increasing rate in a mobile environment, and there is an increment in Wi-Fi access points (APs) deployment (InterDgital 2012). Based on this, WFA that stands for the certification of Wi-Fi products has formed Hotspot 2.0 Specification which is a technical specification that consists of some industry standards (Ericsson 2012).

Connection to an ordinary Wi-Fi hotspot may require subscriber to perform some manual steps (searching for a network, initiating a connection to the network and entering account credentials by launching a web browser) to get the internet access. Although, there are some enhanced solutions such as captive portal they are limited for certain devices and they are not widespread. WFA Hotspot 2.0 Specification aims to support widespread automatic switching to Wi-Fi by driving network interoperability

and standardized network association, authentication, security, sign-up and policy control that is totally transparent to the user in terms of mobile devices. Hotspot 2.0 release 1 has defined capabilities for network discovery and selection, and secure authentication. (Ericsson 2012).

The key enabling protocols for Hotspot 2.0 release 1 are IEEE 802.11u, EAP methods and IEEE 802.11i that run on top of IEEE 802.11. Basically, IEEE 802.11u protocol supports Wi-Fi devices to find out the network capabilities by providing a communication link with Wi-Fi APs. This is performed by the generic advertisement service (GAS) and the access network query protocol (ANQP) that are used by IEEE 802.11u. (Rukus 2013a)

1.1 Motivation

Operators start to leverage Wi-Fi capabilities in all around the world. All mobile operators in Korea have decided to set up a wide Wi-Fi network, China mobile is deploying one million hotspots, AT&T has purchased a large Wi-Fi network, O2 is in a partnership with The Cloud a leading Wi-Fi operator in UK and so on (Transection Network Services 2011). These attempts show the importance of Wi-Fi in case of high data transmissions. By the implementation of Hotspot 2.0 specification, in such Wi-Fi networks, operators are considered to gain in terms of fulfilling the customer demands; mobile, cost effective high data transmission.

Wi-Fi Alliance Hotspot 2.0 Specification is known to be new in the market. Therefore, the research conducted and the information provided by this master thesis is going to be highly substantial to gain WLAN operators.

1.2 Scope of the Research

This thesis work covers WFA Hotspot 2.0 Specification based Wi-Fi network discovery and selection, secure authentication and connectivity, and network element requirements by providing a good understanding of the system functionality. The hardware design and site-implementations are not considered within the scope of this thesis; however, the network architecture deployment framework is proposed in terms of different scenarios. Moreover, WFA Hotspot 2.0 specification is taken under testing in case of different scenarios such as Passpoint functionality check, handover between APs and Roaming between different WLANs.

1.3 Research areas

In this master thesis, there are few key points that are considered to be the main areas of the research.

- Overall System Functionality; the communication flow between UE and WLAN, used protocols/methods and transmission/reception frames will be studied and described to give a good understanding of the system functionality.
- Roaming to commercial networks; except the operator's core network, there will be commercial networks such as iPass, FON, Langaton Tampere, City of Vaasa or any other local operator networks. Possible ways to incorporate these networks, with no user intervention, will be studied to provide the operator to be able to give a global and domestic extension of services based on their agreements with other network operators.
- Authentication process; username/password based a secure authentication type will be investigated and possible implementation based solutions will be introduced.

- Network deployment framework description and core element requirements; network elements will be described and the information based on the requirements for the system adaptation will be provided.
- Testing Phases for different scenarios; Passpoint functionality check, Handover between different Passpoint APs and roaming to a different WLAN will be performed to check the applicability of the system and to be prepared for the future case real implementations.

1.4 Thesis Contribution

The results that are gained through this master thesis will bring several benefits for the company in case of their implementation;

- The company's operations are solely based on fixed line communications. Therefore, the outcomes of this study might lead the company to get into mobile communication service which means gaining more subscribers by providing flexible services.
- Automated and mobile connection experiences for its subscribers, customer delight.
- As the company has landline, also fiber optic lines, implementation of such a wide Wi-Fi network will provide company to give service to mobile operators in terms of off-loading. This undoubtedly means to have a share from mobile operators' market share.
- From the technology point of view, conducting such a research will gain company to keep up with the technological developments in Wi-Fi area.

1.5 Outline of the Thesis

The following chapters stand for the subsequent work that has been done in this master thesis.

Chapter 2

Concentrates on background information related to WLAN (Its standards and architecture) and IEEE 802.11u amendment to have the best understanding to conduct this research. Subsequently, the proposed programs by WFA and WBA associations are introduced. However, this thesis only concentrates on WFA based program/technology that is called as Wi-Fi Alliance Hotspot 2.0 Specification by refereeing to IEEE 802.11u amendment. Moreover, it gives information about Passpoint elements (Beacon & Probe frames and GAS/ANQP) that provide initiation and association of communication between Passpoint UE and Passpoint APs.

Chapter 3

Provides a good understanding about Passpoint network discovery and selection based on beacon frames and ANQP queries. Moreover, recommendations for network and service providers are given in case of deployment.

Chapter 4

First, it gives a short introduction to wireless security and later on it focuses on WPA2-Enterprise Security and different authentication methods in details. Besides, it describes PEAP/MSCHAPv2 based authentication scenario in details.

Chapter 5

Describes the network core elements including UE and explains the requirements for the deployment of the system. Subsequently, ANVIA Passpoint WLAN Architecture is described in details for different functionality scenarios.

Chapter 6

Performs hands on testing in terms of different scenarios such as Passpoint functionality check, handover between ANVIA Passpoint WLAN APs and, Passpoint roaming between ANVIA WLAN and Langaton Tampere WLAN.

Chapter 7

Presents the conclusion for this thesis and gives propositions for the future work.

2 BACKGROUND

This Chapter provides information related to WLAN (Its standards and architecture) including IEEE 802.11u amendment. Subsequently, the proposed programs by WFA and WBA associations are introduced. However, this thesis only concentrates on WFA based program/technology that is called as Wi-Fi Alliance Hotspot 2.0 Specification refereeing to IEEE 802.11u amendment. Moreover, it gives information about Passpoint elements (Beacon & Probe frames and GAS/ANQP) that provide initiation and association of communication between Passpoint UE and Passpoint APs.

2.1 Wireless Local Area Network

LANs arose in the early 1980s to provide sharing of resources and peripherals such as access servers, printers and shared storage devices among PCs, terminals and other distributed computing devices (Pushpendra Kr. V., Shekhar P., Shekhar J. 2011). However, in today's technology, almost all of the communication devices are being produced by having wireless data transmission/reception capabilities. Mainly, such devices which are capable of using wireless technology are equipped to perform network connection with WLAN.

WLAN is a system that uses electromagnetic waves to provide data exchange between mobile end user and operator's wired backbone network that may provide connection to a wider Internet. This provides users the ability of mobility within the coverage area of WLAN. This network type is based on the Institute of Electrical and Electronics Engineers' (IEEE) 802.11 standards that is established in 1991. IEEE and WFA have been in a close coordination to improve the capabilities of Wi-Fi that is abbreviation of Wireless Fidelity; however, it has importance to know that IEEE 802.11 devices are not Wi-Fi unless and until they have been passed under the certification by the WFA (Inter Digital 2012).

2.2 IEEE 802.11 Standards

The 802.11 standard has quite many indices, from how to perform synchronization, to how to configure IR wireless networks, to SS chip rates for dissimilar applications, which perform access to wireless network (Justin Berg 2011). In this part, all the amendments of the standard are not studied; however, the main standards and amendments are handled including IEEE 802.11u which is the core of this research.

IEEE 802.11 is developed by the IEEE LAN/MAN Standards Committee (IEEE 802) in the 2.4GHz and 5GHz unlicensed spectrum bands and it stands for a set of standards for WLAN computer communications. The 802.11 family consists of the over-the-air modulation techniques that are based on the same protocol. Although, 802.11a was the first standard for wireless networking 802.11b was the first widely accepted one, followed by 802.11g and 802.11n. (Kaushik S., Kaushik M. *2012*).

IEEE 802.11a – By using OFDM waveform with different modulation techniques it allows communication up to 54Mbps at 5 GHz operating frequency (IEEE Std 802.11a-1999). The 802.11a causes much less RF interference than others e.g. 802.11b and 802.11g; however, its hardware expenses are higher. Although, the standard provides a high bandwidth a decrease in its effective range occurs because of its high operating frequency that is readily absorbed by physical weaknesses such as walls and other solid objects in their line of sight.

IEEE 802.11b – Uses DSSS waveform with CCK modulation schema it allows communication up to 11 Mbps at 2.4 GHz operating frequency (IEEE Std 802.11b-1999). 802.11b is an extension of the modulation technique that is introduced in the original standard. The increase in throughput and price reduction has leaded this standard to become the most acceptable WLAN technology. Although, it is inexpensive and has a wider coverage area compared to 802.11a it suffers from interference with other devices that functions at the same operating frequency. Microwave ovens, Bluetooth devices, baby monitors and cordless telephones are such devices that cause interference to IEEE 802.11b. Although, it is considered to be possible to mitigate the

condition by limiting the sources of RF interference the problem cannot be eliminated every time (Telecom Regulatory Authority 2003).

IEEE 802.11g – Operates at 2.4GHz, uses OFDM and CCK modulation and it allows communication up to 11 Mbps with CCK modulation and up to 54 Mbps with OFDM (IEEE Std 802.11g-2003). 802.11g is fully backward-compatible with 802.11b. Therefore, this specification provides a considerable increase in data rates and an inexpensive hardware as all the 802.11g equipment were compatible with 802.11b. This standard also suffers from interference that is caused by other devices operating at the same frequency band.

IEEE 802.11n – is an amendment that provides MIMO and an increased bandwidth to the current broadcast sets, IEEE 802.11b and IEEE 802.11g. It allows communication up to 100 Mbps and greater and functions at both 2.4GHz and 5GHz operating frequencies using 20 MHz and 40 MHz channels respectively (IEEE Std 802.11n-2009).

2.3 Wi-Fi Performance and Comparison

Table 1. Wi-Fi Standards Comparison.

	802.11a	802.11b	802.11g	802.11n
Approved	July 1999	July 1999	June 2003	Oct-2009
Max. data rate	54 Mbps	11 Mbps	54 Mbps	600 Mbps
Multiplexing Technique(s)	OFDM	DSSS and CCK	OFDM and CCK	MIMO, DSSS and OFDM
Modulation Technique(s)	PSK or QAM	PSK	Various	Various
Throughput	27	5	22	144
Frequencies GHz	5.15–5.35 5.425–5.675 5.725–5.875	2.4–2.497	2.4–2.497	5 and/or2.4

IEEE 802.11u – The ninth amendment of IEEE 802.11-2007, IEEE 802.11u, which stands for communication protocols between APs and UEs, is new protocol of IEEE

802.11 family that is published on February 25, 2011. IEEE 802.11u supports interworking of WLAN with external networks to provide external authentication, authorization and accounting as well as network selection, encryption, resource management and policy enforcement. (Rukus 2013b).

All IEEE 802.11 standards support the same frame structure and use CSMA/CA that stands for sensing the medium before the transmission of the packets. A brief comparison among the main IEEE standards in terms of technical specifications may be observed in Table 1.

2.4 Legacy WLAN Network Architecture

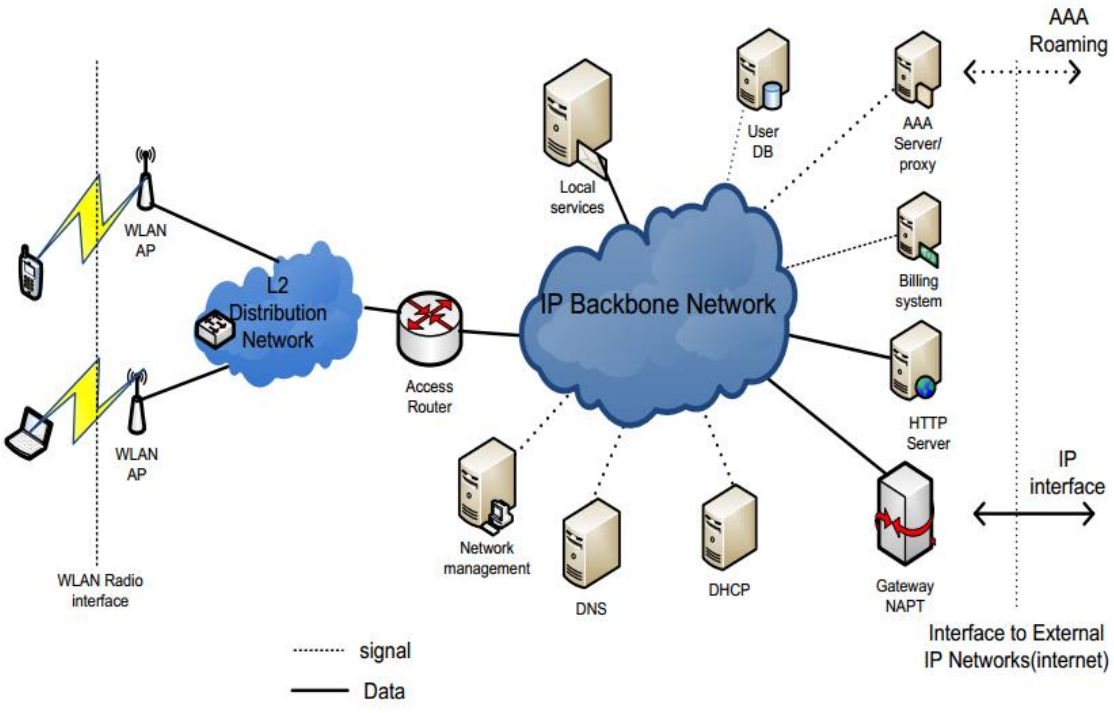

Figure 1. WLAN Network Architecture

The Dynamic Host Configuration Protocol (DHCP) server is required to configure devices connected to a network to provide them communication on that network by using the Internet Protocol (IP). Domain Name Server (DNS) resolves Internet fully

qualified domain name (FQDN) address into IP addresses. For example, www.example.com is a domain name and it is translated to the address 192.0.43.10 (IPv4). Gateway/Network address and port translation (NAPT) is a gateway for external IP networks such as Internet. Generally, the gateway also performs IP network address and port translations to enable the WLAN access network operator to use private-space IP addresses inside the WLAN system and enable access to services available outside IP networks at the same time. Hyper Text Transfer Protocol (HTTP) server may provide local application-level services for accessing users. Accounting data is processed in the billing system server. The local services server is a general box covering services at IP level or above, such as mail servers and local web content. Network management takes care of the management of entire network elements at all layers. It is instrumental in network configuration and monitoring. (Garg 2010).

WLAN AP is generally a layer 2 bridge between IEEE 802.11 and the Ethernet. The WLAN terminal that will be mentioned as UE is typically a personal digital assistant (PDA) or laptop computer that has a built-in WLAN functionality. APs are attached to layer 2 distribution networks such as a switched Ethernet subnet. The layer 2 distribution network may also provide intra-subnet mobility for WLAN terminals. The layer 2 distribution network enables layer 2 connectivity towards the first IP routing device, access router (AR). The basic function of AR is to route user IP packets. (Garg 2010).

IP connectivity and other services require authentication and authorization as a one basic prerequisite via WLAN. For this purpose authentication, authorization, and accounting (AAA) server and user database are required. User data base (DB) is used to store the subscribers' user identities such as login names, shared secrets like passwords, and user profiles. Over the IP backbone network user DB is accessed from the AAA server using lightweight directory access protocol (LDAP) or the user DB is included in AAA server. (Garg 2010).

In legacy WLAN, authentication and authorization is held using Web browsers. After user performs the connection with the AP and initiates a web browser, its first request is directed to a WLAN system HTTP server where the user may enter a login name and

password. At the same time users may be asked to enter their credit card information and make payment for the connection for a limited time.

2.5 WFA: Hotspot 2.0

Wi-Fi Alliance is a global non-profit trade association that enhances the capabilities of WLAN and certifies products whether they reach certain standards of interoperability. WFA launched the Wi-Fi CERTIFIED program, in March 2000, to provide a globally recognized designation of interoperability and quality, and this certification program ensures that Wi-Fi CERTIFIED products will deliver the best user experience.

As the certification process might be costly not every Wi-Fi capable device is submitted for the certification to the WFA and the lack of Wi-Fi CERTIFIED logos does not mean that the device is incapable of functioning properly.

WFA Hotspot 2.0 is developed by WFA to allow UEs to simply identify, select and associate without any user intervention in a highly secure manner and it is called to be the technology lies behind the Wi-Fi CERTIFIED Passpoint program that points out the operator and user needs. The Wi-Fi CERTIFIED Passpoint program is created to test and confirm interoperability between devices from different vendors. (Rukus 2013a).

Due to Passpoint, UEs are allowed to discover information about the hotspots before performing the association process to identify and prioritize the hotspots according to their needs and subsequently perform authentication and get connected to the desired service.

The main technical details are as follows:

- Leverages 802.11u.
- Newly introduced information elements in beacons and probe responses.
- New GAS/ANQP protocol to perform pre-association queries between UE and AP.

- Covers SIM and non-SIM devices (e.g. cellphones, tablets and laptops).
- Utilizes 802.1X as the core authentication protocol.

2.5.1 Reference Architecture

In case of Passpoint UEs with no U(SIM), network discovery and authentication occurs as follows. First, Passpoint APs emit beacon frames that indicate Hotspot 2.0 indication to be detected by UE. Based on the received beacon frames, UE queries to ANQP server for NAI realm list, roaming consortium OIs etc. Subsequently, APs answer to the query with required ANQP elements and based on this UE functions to match the realms and OIs received against its list of credentials and preferred networks. In case of finding a match, UE automatically connects to AP and performs IEEE 802.1X authentication to the Home AAA server by using EAP-TLS, EAP-TTLS/MS-CHAPv2 or PEAP/ MS-CHAPv2. (Wi-Fi Alliance 2012a).

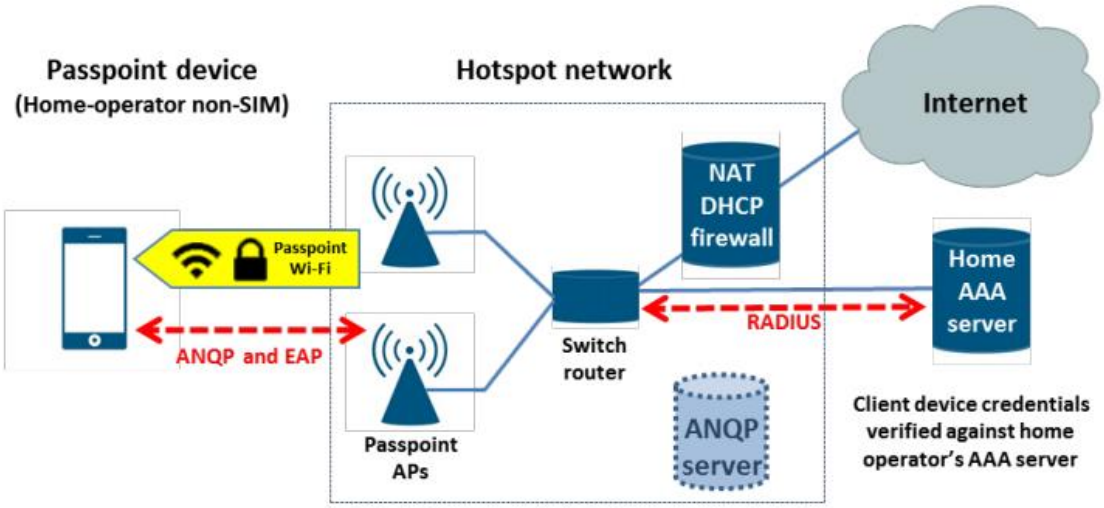

Figure 2. Passpoint Hotspot 2.0 reference architecture: non-SIM (Wi-Fi Alliance 2012a).

2.6 WBA: Next Generation Hotspot

Wireless Broadband Alliance NGH that is a program created by mobile industry aims to assist mobile operators to offload mobile data traffic via Wi-Fi hotspots and fixed

backhaul. It is based on WFA hotspot 2.0 specifications supports UE for automatic and secure interoperable authentication with hotspots by using its SP credentials. The increasing number of Wi-Fi capable devices requiring high BW that cellular networks remain weak to meet the demand has pushed mobile providers to offload the data traffic from their cellular networks to WLAN. (Transection Network Services 2011).

2.6.1 Reference Architecture

In case of Passpoint UEs with SIM or USIM, network discovery and authentication occurs as follows. First, Passpoint AP emits beacon frame that indicates Hotspot 2.0 indication to be detected by UEs. Based on received beacon frame, UE queries ANQP server for 3GPP cellular network information and roaming consortium OIs. Subsequently, AP answers to the query with required ANQP elements and based on this UE functions to match the 3GPP cellular network information and OIs received against its list of credentials and preferred networks. In case of finding a match, UE automatically connects to AP and performs IEEE 802.1X authentication to the Home AAA server by using EAP-SIM or EAP-AKA. Finally, Home AAA server communicates with HLR by using MAP. (Wi-Fi Alliance 2012a).

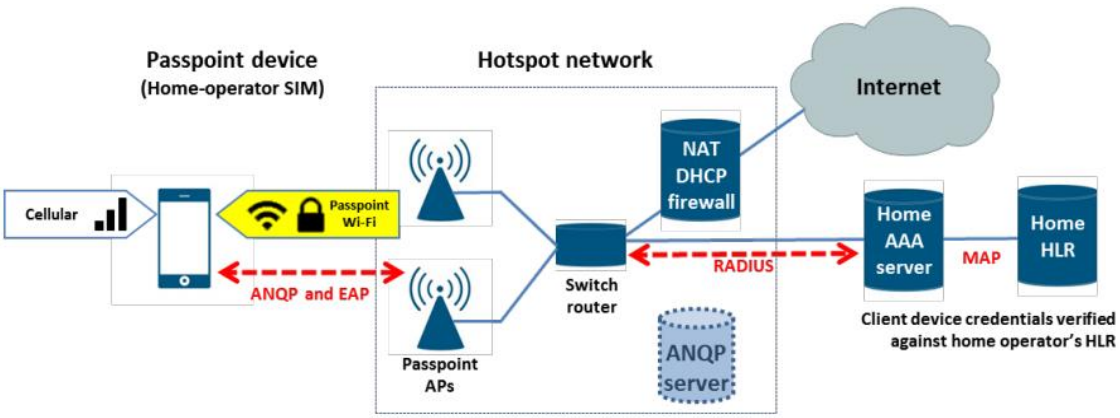

Figure 3. Passpoint Hotspot 2.0 reference architecture: SIM (Wi-Fi Alliance 2012a).

2.7 Passpoint Elements

Passpoint may be considered in there phases; Advertising its services in beacon or probe response frames, the communication of ANQP queries and selection of AP for user authentication based on gathered information.

2.7.1 Service Advertising

Basing on the information provided to the UEs in beacon and probe response frames UEs may be able to start the association process. A scan allows the UEs to recognize a list of Passpoint capable APs that answers to their needs of connection. APs advertise their capabilities to UEs in two ways, passive scanning and active probing.

The data flow between UE and APs in a pre-association state has advantages:

- The necessary information about the IEEE 802.11 infrastructure is provided to UEs to perform the association process with the proper AP. It is considered to be more efficient than associating with an AP before collecting information about it and deciding whether to stay connected or not.
- A UE may gather information from multiple networks in parallel. By this way, it is aimed to select the most appropriate AP.
- UE may perform the same process in case of associating with an AP that is from a different IEEE 802.11 infrastructure by having a proper SSP roaming agreement.

Passive Scanning **–** By listening to beacon frames that are periodically sent by APs (100 millisecond), UEs try to discover the wireless networks that cover its current location. To perform this action, UE prepares a list of channels and listens to beacon frames transmitted on each of these channels. Passive scanning is generally used over active probing by UEs to save the battery life as they do not transmit any data but only listening the beacons.

Active scanning **–** Generation of probe request frames followed by the process of received probe response frames are two steps that are performed in active scanning. UEs

use active scanning to search for the surrounding wireless networks to locate a compatible one and they perform an active scan by emitting a probe request frame that includes wildcard SSID and an interworking element with specified access network type subfield.

User may set his preference of network type subfield by tapping on an icon, e.g. airport, shopping, museum or emergency call, on Wi-Fi capable device. This choice will provide the UE to make an active search for the desired network type and connection accordingly. In response to a probe request frame, AP replies back to the UE with a probe response frame including information that is similar in a beacon frame.

2.7.2 GAS

GAS is an IEEE 802.11u service which handles the transportation of higher-layer (layer 2) advertisement frames between APs and UE or between a server in an external network and UE. By those higher-layers advertisement services, UEs are enabled to discover information availability based on the desired network services provided by SSPNs or other external networks through the AP, before the association to the wireless LAN. This is achieved by using the Public Action management frames. Separately addressed Public Action frames should be used to deliver GAS messages. If the protection of management frame is negotiated GAS messages shall be transmitted using individually addressed Protected Dual of Public Action frames instead. (IEEE 802.11 2012).

An advertisement protocol that exists in the advertisement protocol element is transported by GAS if Advertisement Protocol ID is added in the Advertisement Protocol element in a Beacon or Probe response frame.

A GAS query request is transmitted by a UE in a GAS initial request frame and according to this AP provides the GAS Query Response or information on how to receive the GAS Query Response in a GAS Initial Response frame. The GAS query response is required to be transmitted in a single GAS initial response frame or in one or

more than one GAS comeback response frames but not split between them. (IEEE 802.11 2012).

Depending on the large information contained in frames GAS message delivery process may vary (Figure 4-6).

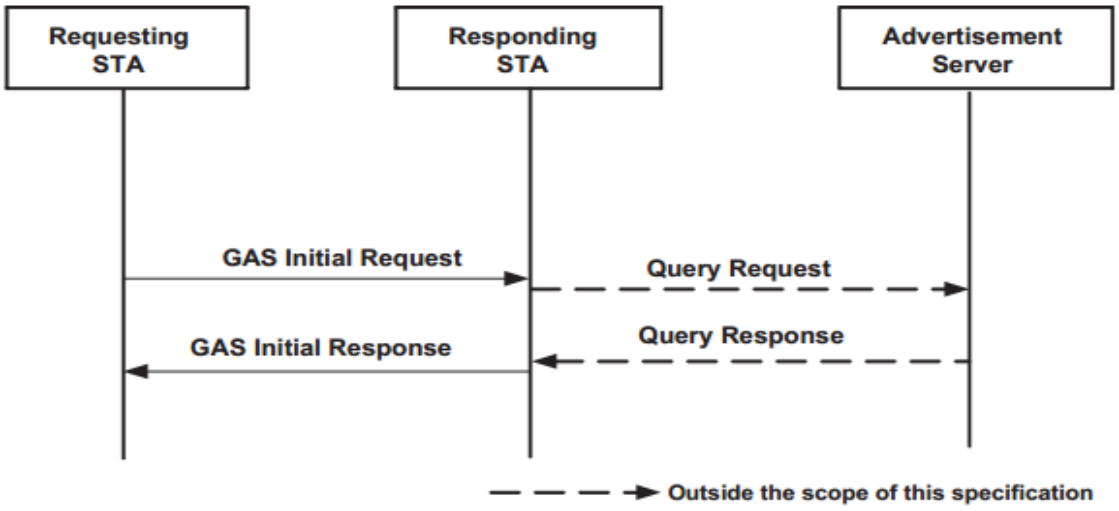

Figure 4. GAS message sequence (IEEE 802.11 2012).

GAS information exchange seen in sequence diagram in Figure 4 indicates that the information requested in GAS initial request is not large in size to be delivered to UE in one MMPDU. Requesting STA (UE) makes the GAS initial request to responding STA (AP) and based on this AP delivers the query request to advertisement server to get the required information in query response to answer to UE with GAS initial response.

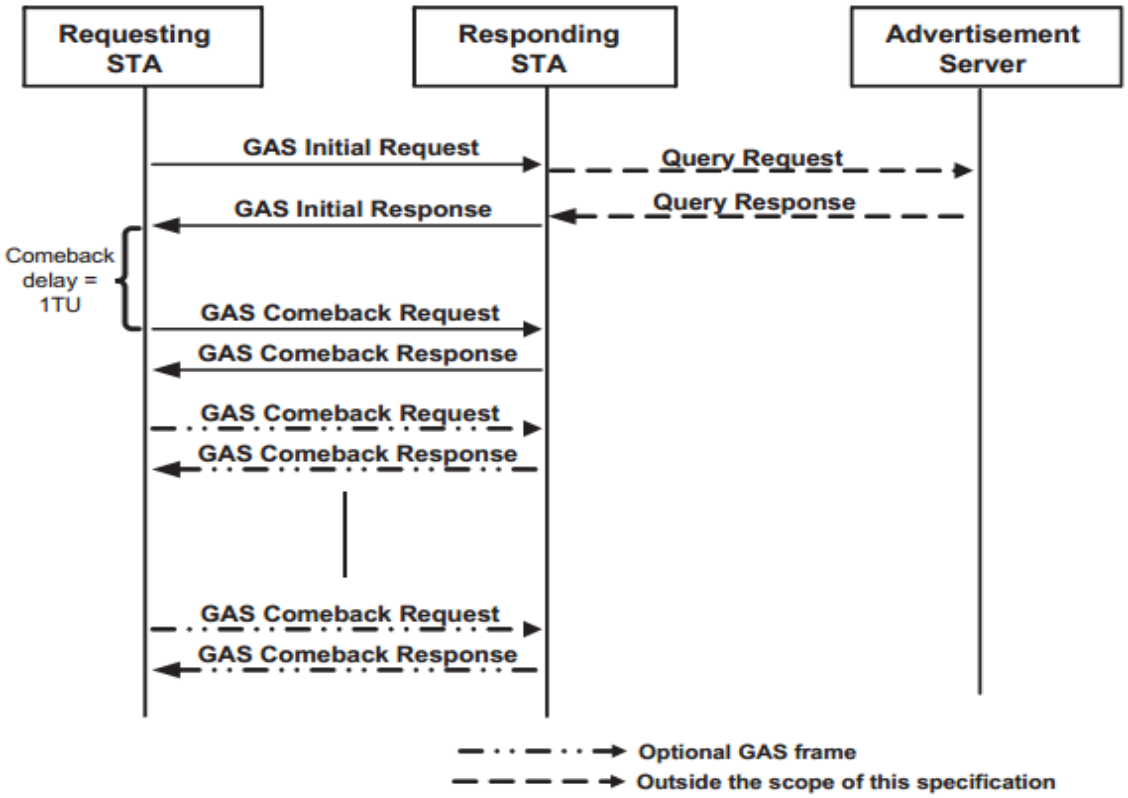

Figure 5. GAS message sequence with GAS fragmentation with no pause for server response (IEEE 802.11 2012).

If the GAS Query Response is too large to fit in one MMPDU, GAS fragmentation is used to deliver the required information (Figure 5). Here GAS initial response informs UE about the comeback delay and the number of frames to be delivered. Due to the number of GAS fragments required to deliver the information GAS comeback request and GAS comeback responses are performed. 1 TU that is defined in comeback delay by 802.11 as 1024 microseconds but the range may vary from 1 millisecond to 30 seconds.

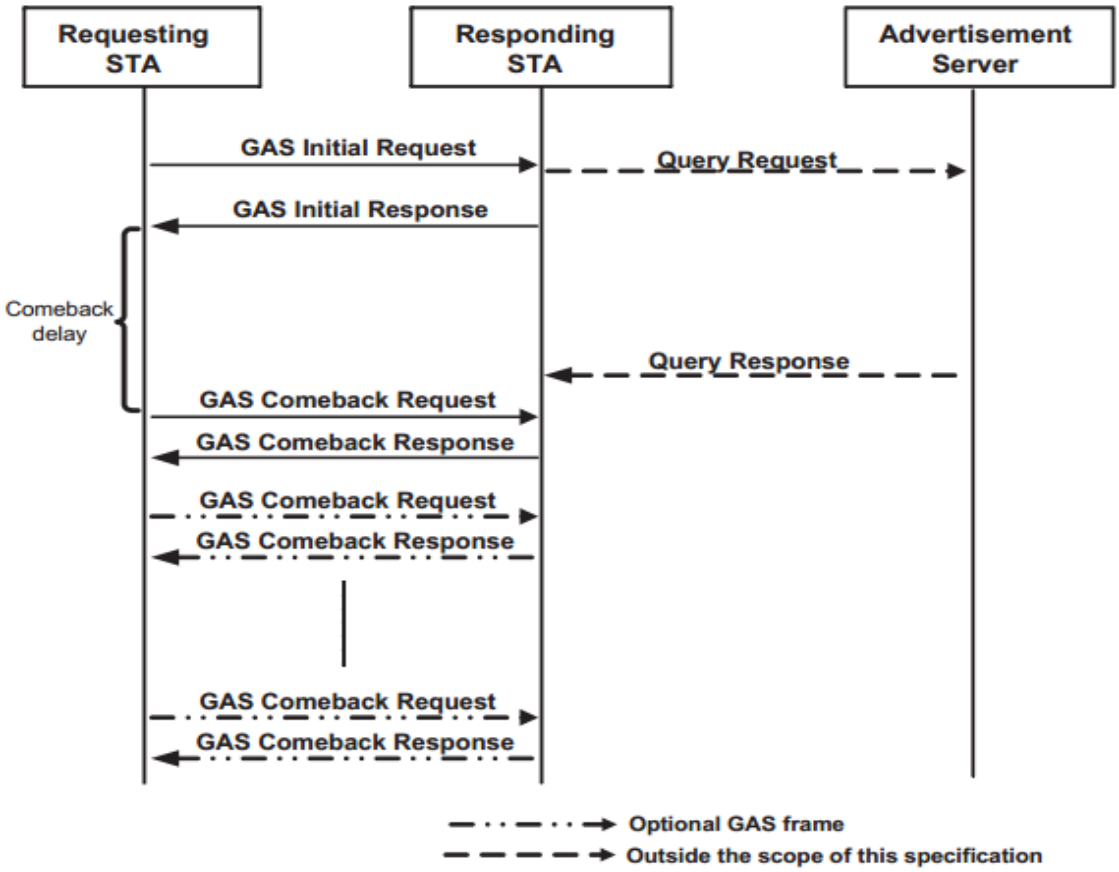

Figure 6. GAS message sequence with GAS fragmentation and with pause for server response (IEEE 802.11 2012).

The sequence diagram seen in Figure 6 is similar to the one in Figure 5; however, when query response is received after sometime by AP from the advertisement server then AP informs the UE to comeback in X seconds and the rest of the information flow is same as it is in Figure 5.

2.7.3 ANQP

ANQP, a new pre-association protocol, is a key innovation in Passpoint and it is significantly faster than establishing authentication before discovering the capabilities of the hotspot by saving the battery life. Beacon and probe response in pre-association are limited in discovery of the capabilities of hotspots. Therefore, a new extended protocol for capability discovery was necessary to be invented that is called ANQP.

ANQP queries are delivered inside GAS; however, GAS and ANQP are used interchangeably. (Aruba 2011).

The Access Network Query Protocol (ANQP) is the query and response protocol that is initiated by UE to automatically discover and select an available and suitable AP (InterDgital 2012). By using ANQP, UE may discover wide information including hotspot operator's domain name, roaming partners accessible via the AP along with their credential type and EAP methods, IP access type availability and so on. Information based on ANQP elements is given in the network discovery and selection chapter in more details.

A general ANQP element format consists of 2 octet info ID field, a 2 octet length field and a variable-length element-specific Information field. Each element has a unique info ID which means that info ID defines and differentiates the frames to be correctly processed at both AP and UE sides. Length field specifies the length of information field in octets. (IEEE 802.11 2012).

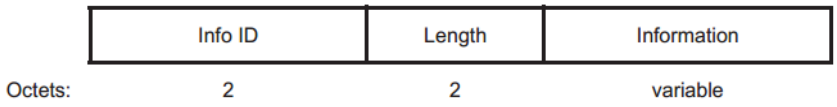

Figure 7. ANQP element format

3. NETWORK DISCOVERY AND ASSOCIATION

3.1 Beacon frame Elements

To indicate their presence and transmit information elements to UEs, APs periodically (100ms) broadcast beacon frames. A general beacon frame format may be observed to be consisted of MAC header, frame body and FCS (Figure 8). In this part, the fields that contain information elements are studied.

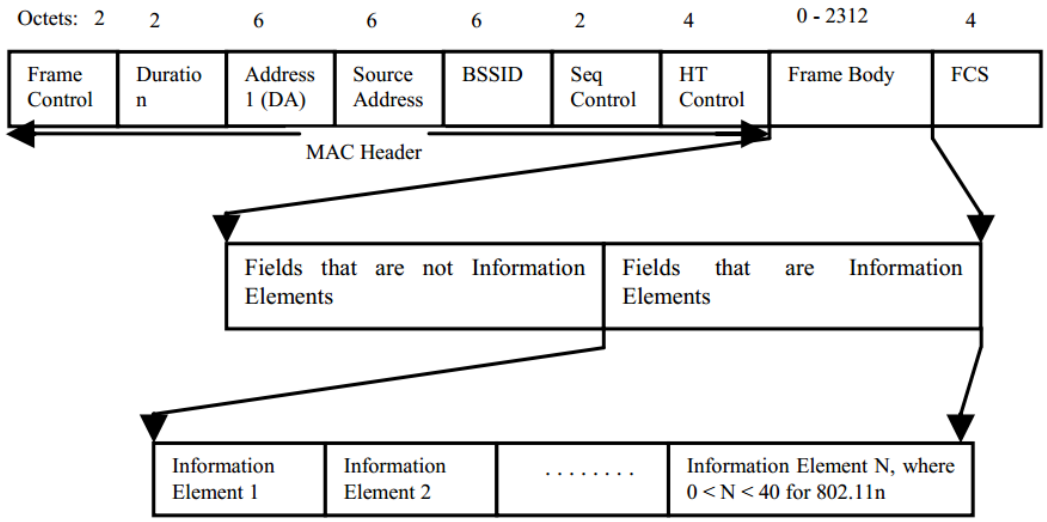

Figure 8. Beacon frame format (Gupta V., Rohil M. K. 2012).

A general information element format consists of 1 octet Element ID field, 1 octet Length and a variable-length element-specific Information parts (Figure 9). Each element has a unique Element ID which means that Element ID defines and differentiates the frames to be correctly processed at both AP and UE sides. Length field specifies the length of information field in octets. (IEEE 802.11 2007)

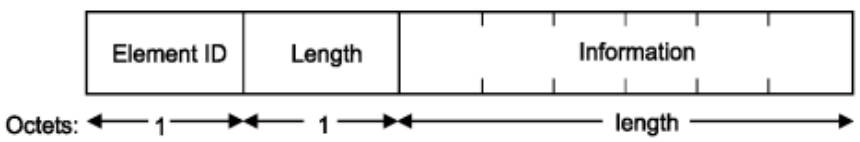

Figure 9. Information element format (IEEE 802.11u 2011).

Table 2 presents a set of elements that are added to IEEE 802.11-2012 standard as the amendment of 802.11u. Here, Element ID values and Length, in octets, are also presented.

Table 3. Beacon Frame Elements (IEEE 802.11u 2011).

Information element	Element ID	Length (in octets)	Extensible
Interworking (see 7.3.2.92)	107	3, 5, 9, 11	
Advertisement Protocol (see 7.3.2.93)	108	variable	
Expedited Bandwidth Request (see 7.3.2.94)	109	3	
QoS Map Set (see 7.3.2.95)	110	18 to 60	Yes
Roaming Consortium (see 7.3.2.96)	111	variable	Yes
Emergency Alert Identifier (see 7.3.2.97)	112	10	
Reserved	113 ~~107~~ –140 and 143 – 220		

3.1.1 Interworking information element

Interworking service capabilities are presented in Interworking information element. 1 octet Element ID, 1 octet Length, 1 octet Access Network Options, 0 or 2 octets Venue info and 0 or 6 octets HESSID fields (Figure 10).

	Element ID	Length	Access Network Options	Venue Info (optional)	HESSID (optional)
Octets:	1	1	1	0 or 2	0 or 6

Figure 10. Interworking element format (IEEE 802.11u 2011).

Access Network Options

The format of Access Network Options field is shown in Figure 11. In the probe request frame UE sets B4-B7 to 0, in (Re)association request frames UE sets B4-B6 to 0 and

sets B7 to 1 in case of indicating that higher layer unauthenticated emergency services are reachable and 0 otherwise. (IEEE 802.11u 2011).

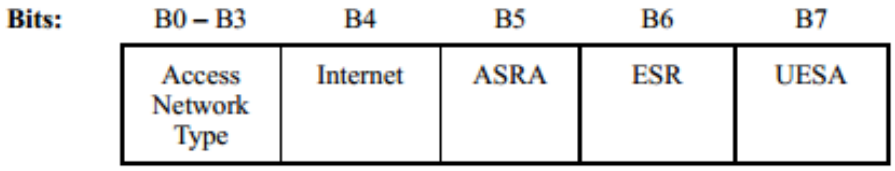

Figure 11. Access Network Options format (IEEE 802.11u 2011).

AP sets ANT to advertise this information to UE and UE use the information provided in ANT when making decision in selection of hotspots. Hotspot operator is expected to configure the ANT according to the type of the hotspot which is typically may be a chargeable public network or free public network (Wi-Fi Alliance 2012). A list of ANTs are provided in IEEE Std 802.11u (IEEE 802.11u 2011).

Bit 4 stands for the Internet available field in the Interworking information element is included in the IEEE 802.11u interworking element present in beacon and probe response frames in Passpoint APs. AP sets this bit to 1 if there is Internet connection available at AP; otherwise it sets this field to 0; however, setting B4 to 0 does not mean that there is no Internet connectivity, it is only unspecified whether Internet access is available at a hotspot (IEEE 802.11u 2011). The reason that Internet would not be available is because hotspot operator may provide a limited Wi-Fi access to locally available content such as museums.

Additional Step Required for Access, ASRA, is assigned to bit 5. AP sets this bit to 1 if there is need for a further step to access the network. In case of setting this bit to 1, network authentication type information provides a list of authentication types for Internet access; however, in some cases it is set to 0 meaning that there is no need for authentication such as in museums.

AP sets B6 to 1 if emergency services are reachable through the AP; otherwise it is set to 0 which indicates that the availability of ESR is unspecified.

Bit 7 stands for UESA field. Assigning 0 to this field means that there is no UESA is reachable through the AP and opposite situation occurs when it is assigned to 1. Simply it means that if the UE does not have credentials for the AP and UESA is set to 1 by AP then UE will have the ability to reach emergency services.

The Venue Info field

The Venue Info field consists of venue group and venue type and it is a 2 octet field (Figure 12). These both subfields are one octet each, and hotspot operator shall configure them accordingly from tables X1 and X2 provided in appendix A (IEEE 802.11u 2011).

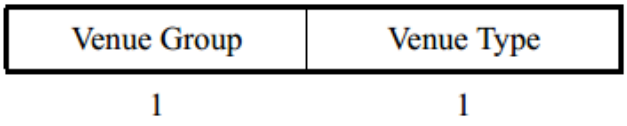

Figure 12. Venue Info field format (IEEE 802.11u 2011).

HESSID

In legacy Wi-Fi deployments, two APs having the same SSID considered to be from the same WN and they are considered to be from different WN in case of having different SSIDs as SSIDs are not globally managed. Therefore, it is highly possible that same SSID belong to two APs from different WNs. Due to HSSID, UEs are able to detect this situation. Even if two APs have the same SSID from different WNs they will have different HSSIDs. (Wi-Fi Alliance 2012).

The HSSID is a globally unique 6-octet MAC address that identifies homogenous ESS. HSSID value should be assigned same with one of the BSSIDs in homogenous ESS and all the APs in WN are required to be configured to the same HSSID value (Wi-Fi Alliance 2012) (IEEE 802.11u 2011). Although, HSSID undertake the responsibility for the identification of the WN SSID are still needed for interworking with legacy devices. Moreover, to provide handoffs between APs within a hotspot the SSID is necessary.

3.1.2 Advertisement Protocol element

Advertisement Protocol element holds information to define a specific advertisement protocol and its advertisement control. Simply, this element Provides IDs for advertisement protocols supported by the Wi-Fi network and most importantly indicates that hotspot supports GAS/ANQP. The length field is one octet and it holds the total length of the Advertisement Protocol Tuple fields (Figure 13).

	Element ID	Length	Advertisement Protocol Tuple # 1	Advertisement Protocol Tuple # 2 (optional)	...	Advertisement Protocol Tuple # n (optional)
Octets:	1	1	variable	variable		variable

Figure 13. Advertisement Protocol element format (IEEE 802.11u 2011).

Advertisement protocol tuple is consisting of Query response info and advertisement protocol ID (Figure 14).

	Query Response Info	Advertisement Protocol ID
Octets:	1	variable

Figure 14. Advertisement Protocol Tuple format (IEEE 802.11u 2011).

Query response info consists of Query Response Length Limit (B0-B6) and Pre-Association Message Exchange BSSID Independent (B7) (Figure 15).

Bits:	B0 – B6	B7
	Query Response Length Limit	PAME-BI

Figure 15. Query Response Info format (IEEE 802.11u 2011).

QRLL defines the total amount of the octets that AP will emit in GAS Initial Response action frame or GAS Comeback Response action frame(s) and it is encoded as an

integer number of 256 octet units. It is probable that QRLL is set to a value larger than maximum MMPDU length which causes to query response to emit more than one MMPDU. In this case, APs use GAS Query Fragment Response ID to inform the UEs (the requesting) about the GAS fragment number of the transmitted frames so that UE will receive all the fragments accordingly. (IEEE 802.11u 2011).

Pre-Association Message Exchange BSSID Independent (PAME-BI) bit is kept for UEs and it is to indicate whether AS's query response is independent of BSSID that is used to exchange GAS frame. It is set to 1 to specify that query response is BSSID independent and opposite way when it is set to 0.

The advertisement protocol ID is a variable length field that is chosen from the following table.

Table 4. Advertisement protocol ID definitions (IEEE 802.11u 2011).

Name	Value
Access Network Query Protocol (ANQP)	0
MIH Information Service	1
MIH Command and Event Services Capability Discovery	2
Emergency Alert System (EAS)	3
Reserved	4 – 220
Vendor Specific	221
Reserved	222 – 255

ANQP provides data retrieval from an AS. MIH information service supports data retrieval from a data repository. MIH Command and Event Services capability supports discovery abilities of command and event service entities in an AP or an external network. EAS provides the network to broadcast emergency notifications from an external network to UEs. EAS uses the message format as defined in OASIS EDXL. Vendor specific information element carries nonstandard information which means the information that is not defined in standard.

	Element ID	Length	OUI	Vendor-specific content
Octets:	1	1	3	n-3

Figure 16. Vendor Specific information element format (IEEE 802.11-2007).

3.1.3 Expedited Bandwidth Request information element

The Expedited Bandwidth Request information element is transmitted in an ADDTS request frame having a TSPEC element from a UE to an AP and describes the use of a traffic stream for the BW request (IEEE 802.11u 2011). The ADDTS frames are used to carry TSPEC to set up and maintain TSs (IEEE 802.11u 2011).

	Element ID	Length	Precedence Level
Octets:	1	1	1

Figure 17. The Expedited Bandwidth Request information element (IEEE 802.11u 2011).

When the controller receives this request, it attempts to facilitate the urgency of the call in any way possible without potentially altering the quality of other TSPEC calls that are in progress.

When the controller receives an emergency call, it tries to provide an urgent connection without potentially decreasing the quality of other TSPEC calls that are in progress (Cisco 2000). First responder (public) represents government agencies related connections and first responder (private) can be considered as individuals or companies (Table 5).

Table 6. Precedence Level field description.

Precedence level value	Description
0 – 15	Reserved
16	Emergency call, defined in NENA 08-002 [B51]
17	First responder (public)
18	First responder (private)
19	MLPP Level A
20	MLPP Level B
21	MLPP Level 0
22	MLPP Level 1
23	MLPP Level 2
24	MLPP Level 3
25	MLPP Level 4
26 – 255	Reserved

Other voice networking technology providers such as 3GPP, ITU and other proprietary signaling protocols provides MLPP services which is used to deliver differentiated levels of consumer services (IEEE 802.11u 2011).

3.1.4 QoS Map Set information element

This element is transmitted from AP to UE in QoS Map configure frame or (Re)association response frame. This element provides higher layer priority mapping from the DSCP field that is used with IP according to the user priorities defined by transmission of data frames (IEEE 802.11u 2011).

	Element ID	Length	DSCP Exception #1 (optional)	...	DSCP Exception #n (optional)	UP 0 DSCP Range	UP 1 DSCP Range	UP 2 DSCP Range	...	UP 7 DSCP Range
Octets:	1	1	2		2	2	2	2		2

Figure 18. QoS Map Set element description (IEEE 802.11u 2011).

The length field value is assigned according to the number of DSCP exceptions used in the frame. Basically, it will be set to 16+2n. The maximum number of adding DSCP exception fields into the frame is 21; however, they might not be used by operator.

	DSCP Value	User Priority
Octets:	1	1

Figure 19. DSCP Exception format (IEEE 802.11u 2011).

The DSCP value is in the range from 0 to 63, or 255; the User Priority value is from 0 to 7. UE first tries to match the DSCP value to a DSCP exception field in the frame and uses UP from the equivalent UP in the same DSCP exception field (e.g. DSCP exception #3, UP 3 Range) if no match is found then UE tries to match it with UP n DSCP Range field except n=0. If those two attempts fail then UE uses a UP of 0. A unique DSCP value is assigned to each DSCP exception field.

	DSCP Low Value	DSCP High Value
Octets:	1	1

Figure 20. DSCP Range description (IEEE 802.11u 2011).

The DSCP Range field corresponding to each of the 8 user priorities has a value between 0 and 63 inclusive, or 255. DSCP range of user priorities do not overlap. DSCP high value is larger than or identical to the DSCP low value and if they are same then the related UP is not used.

3.1.5 Roaming Consortium information element

Information that provides a list of the Roaming consortium and/or SSP that are roaming partners of the hotspot SP and that are reachable from the Passpoint AP is consisted in Roaming consortium information element (IEEE 802.11u 2011). For a large Hotspot SP it is mandatory to register for an OI; however, it could be optional for smaller SP (e.g. hotels) (Wi-Fi Alliance 2012a).

	Element ID	Length	Number of ANQP OIs	OI #1 and #2 Lengths	OI #1	OI #2 (optional)	OI #3 (optional)
Octets:	1	1	1	1	variable	variable	variable

Figure 21. Roaming Consortium information element format (IEEE 802.11u).

One octet length value includes 2 plus the total sum of octets in OI fields. In this frame, there will be a total of three OIs. Depending on the number of ANQP OIs filed value the number of additional roaming consortium OIs is defined. Assigning a value 0 to this field means there will be no additional OIs in response to an ANQP query and a value of 255 indicates that there will be 255 or more additional OIs via ANQP.

Bits:	B0 – B3	B4 – B7
	OI #1 Length	OI #2 Length

Figure 22. OI #1 and #2 Lengths field format (IEEE 802.11u).

The length in octets of the OI #1 and OI #2 fields in Roaming Consortium information element format frame are assigned to OI #1 and #2 Lengths fields with respected to the order. If there is not OI #2 then the value is assigned to 0. In case of having the third OIs, the length of OI #3 is calculated as following formula:

$$The\ length\ of\ OI\ \#3 = Length\ field - (2 + subfield\ length(OI\ \#1 + \ OI\ \#2))$$

The OI field identifies a single SP or a roaming consortium list that is consists of a group of SSPs having inter-SSP roaming agreements. It is recommended for national and international SPs to have an OI by WFA.

The main use cases for OIs are as follows:

- Only three OIs can be placed in a beacon frame and in case if any of those OIs is recognized by the UE, then ANQP does not need to be performed to determine

whether UE can authenticate to the hotspot. This can provide UE to save the battery life as it will not make extra query for authentication discovery.

- By the use of OIs, SPs may provide different subscription levels (e.g., gold, silver, bronze). While gold users might have access rights to all APs, bronze users might not have access right to connect to APs that are in premium locations.

3.1.6 Emergency Alert Identifier information element

The Emergency Alert Identifier information element provides information (Alert Identifier Hash) that may be used by UE for the verification of EAS messages that are available at that moment. UEs evaluate whether EAS messages have been previously received from APs due to hash and based on this information UEs decide whether to download it from network or not. AIH is a 8-cotet field and its value is assigned by the HMAC-SHA1-64 hash algorithm operating on the EAS message.

	Element ID	Length	Alert Identifier Hash
Octets:	1	1	8

Figure 23. Emergency Alert Identifier information element format (IEEE 802.11u 2011).

3.2 ANQP Information Elements

3.2.1 SP Identification and Authentication Methods

NAI Realm List

Via an AP, it provides a list of NAI realms related to SSPs or any other entities whose services are available (Figure 24) and there is optionally a list of one or more than one EAP method subfields included in case of each NAI realm to provide authentication

(IEEE 802.11u 2011) (Wi-Fi Alliance 2012). NAI realm determines the proper domain or authentication server to authenticate the UEs, and accordingly UEs makes a decision to authenticate to its preferred network (Rukus 2013b).

	Info ID	Length	NAI Realm Count	NAI Realm Data #1 (optional)	NAI Realm Data #2 (optional)	. . .	NAI Realm Data #n (optional)
Octets:	2	2	2	variable	variable		variable

Figure 24. NAI Realm list format (IEEE 802.11u 2011).

NAI realm list is supposed to be configured as follows:

- The realms of all the roaming partners accessible through the Passpoint AP including the home SP should be added to the list.
- Although, PLMN ID appears in 3GPP cellular network information ANQP element it can also be added to NAI realm list.

For example,

wlan.mnc410.mcc310.3gppnetwork.org and epc.mnc410.mcc310.3gppnetwork.org

- The EAP method authentication parameter type is required to be configured according to Table 7 to support UEs that do not know what EAP methods are used by a given SP.
- If the UE is associated with credentials by the SP the UE does not necessarily need to use the data provided in the EAP method list section of the NAI realm list.

User preferences and policy may be predefined to decide whether to connect to a Passpoint AP or non-Passpoint AP in case that they are both available in the coverage area. More information about this element configuration is provided in IEEE std. 802.11u.

Table 8. NAI Realm list format (IEEE 802.11u 2011).

Authentication information	ID	Description	Length (octets)
Reserved	0		
Expanded EAP Method	1	Expanded EAP Method Subfield	7
Non-EAP Inner Authentication Type	2	Enum (0 - Reserved, 1 - PAP, 2 - CHAP, 3 - MSCHAP, 4 - MSCHAPV2)	1
Inner Authentication EAP Method Type	3	Value drawn from IANA EAP Method Type Numbers	1
Expanded Inner EAP Method	4	Expanded EAP Method Subfield	7
Credential Type	5	Enum (1 - SIM, 2 - USIM, 3 - NFC Secure Element, 4 - Hardware Token, 5 - Softoken, 6 - Certificate, 7 - username/password, 8 - none*, 9 - Reserved, 10 - Vendor Specific) *none means server-side authentication only	1
Tunneled EAP Method Credential Type	6	Enum (1 - SIM, 2 - USIM, 3 - NFC Secure Element, 4 - Hardware Token, 5 - Softoken, 6 - Certificate, 7 - username/password, 8 - Reserved, 9 - Anonymous, 10 - Vendor Specific)	1
Reserved	7–220		
Vendor Specific	221	Variable	variable
Reserved	222–255		

Roaming Consortium List

The information presented in this list is same as the information presented in Roaming Consortium information element in beacons and probe responses; however, in case of need, the number of OIs is not limited to 3 in this ANQP element (Rukus 2013b).

	Info ID	Length	OI Duple #1 (optional)	OI Duple #2 (optional)	…	OI Duple #N (optional)
Octets:	2	2	variable	variable		variable

Figure 25. Roaming Consortium list format (IEEE 802.11u 2011).

In this ANQP element, there might be zero or any number of OI duples depending on hotspot operator's configuration. If there has been added any OIs in the roaming consortium information element in beacons and probe responses are included in this element, too.

3GPP Cellular Network Information

This element is consisting of cellular information such as identifying the Public Land Mobile Network (PLMN) ID that covers the Mobile Country Code (MCC) and Mobile Network Code (MNC) of the mobile operator to assist a 3GPP UE to select an AP to connect 3GPP networks (IEEE 802.11u 2011) (Rukus 2013b). This ANQP information element is for the clients with a cellular subscription (SIM or USIM) to use PLMN ID to figure out whether hotspot provides authentication with the client's mobile operator (Rukus 2013b).

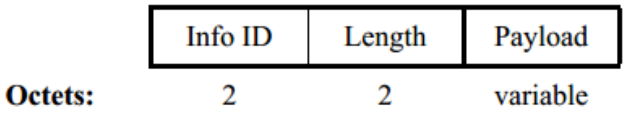

Figure 26. 3GPP Cellular Network information format (IEEE 802.11u 2011).

3.2.2 Hotspot Identification

Venue Name Information

The venue name information ANQP element (Figure 27) informs UE about additional information related to hotspot's location. Hotspot operator sets all the APs with the same venue name in a venue; however, different venues that have Wi-Fi access from the same operator may have different venue names even if they share the same SSID (e.g., two coffee shops sharing the same SSID but having different venue names). Moreover, venue names may be listed in many languages by hotspot operators and this specification may be displayed by UE to user due to preferred language in case of availability. (Wi-Fi Alliance 2012). For instance, in a hotel X, there are many SSIDs that your device may detect such as hotel X floor1, hotel X floor2 and so on. By the implementation of WFA Hotspot 2.0, there is only one SSID and the AP location information is provided in Venue Name Information that provides a simple way of Wi-Fi connection.

	Info ID	Length	Venue Info	Venue Name Duple #1 (optional)	Venue Name Duple #2 (optional)	…	Venue Name Duple #N (optional)
Octets:	2	2	2	variable	variable	…	variable

Figure 27. Venue Name information format (IEEE 802.11u 2011).

Because of the UE's location the connection to a specific AP might have an important value as there might be offered some special services through an AP. For instance, a fan might want to make sure to make a connection to stadium Wi-Fi rather than a café next door. (Aruba Networks, Inc. 2011). In case of manual hotspot selection, UE may make an ANQP query to obtain venue name information and this information is displayed on UE based on its implementation. The Venue Info field is same as it is defined in beacons and probe response frames.

Domain Name List

This element provides one or more than one domain names of the entity that operates the AP. This element has a high importance as it identifies the AP's operator. Due to this information UE knows whether it is in the coverage of home or visited network (Rukus 2013b).

	Info ID	Length	Domain Name field #1 (optional)	Domain Name field #2 (optional)	. . .	Domain Name field #N (optional)
Octets:	2	2	variable	variable		variable

Figure 28. Domain Name list format (IEEE 802.11u 2011).

Hotspot operator may have multiple domain names that identify it. "For example, the domain names wlan.mnc410.mcc310.3gppnetwork.org, att.com, and attwireless.com all refer to the same SP, AT&T. All three will be contained in the domain name list ANQP element." (Wi-Fi Alliance 2012). Hotspot operators are expected to have at least one domain name and this domain name is configured in the domain name list. At the selection phase of the APs, UE chooses the AP that is operated by its home network

operator; however, this selection may differ if the priority is given to other APs in case of different conditions maybe by user preferences or operator's policy.

After the reception of the domain name list from the AP, UE tries to match the FQDN such as "anvia.fi" in its credential as a suffix match to the domain names in this list to see whether it is going to connect an AP operated by its home SP. An UE whose home SP is ANVIA will consider any AP with a domain name that has anvia.fi as a suffix (e.g., amarillo.anvia.fi) is operated by its home SP.

In case that the SP's domain name is not in the list but in the realm list, then UE that makes the association based on that SP is going to be considered to be roaming.

Hotspot Operator Friendly Name

This element is configured in Passpoint AP by hotspot operator to provide UE the operator friendly name in many languages. UE may access the hotspot operator friendly name via GAS/ANQP queries to guide user during the manual hotspot selection or to provide operator name to the user. The capability of displaying the information in this element is depended on the implementation of the UE.

3.2.3 Network Characteristics ANQP Elements

IP Address Type Availability Information

By this element, UE is provided the information about the availability of IP address version and type that could be assign to it in case of a successful authentication to the network. IP address field is consisting of IPv4 and IPv6 information (Figure 29).

	Info ID	Length	IP Address
Octets:	2	2	1

Figure 29. IP Address Type Availability information (IEEE 802.11u 2011).

In case of network selection process this element plays a vital role such as that a EU with only an IPv4 stack joins to an AP supporting IPv4 and a UE that supports IPv6

stack may prefer to connect to a hotspot which provides IPv6 connectivity if there is any available.

This information is required to be configured by the hotspot operator to indicate the IP address configuration of the WAN router, the DHCP server and the firewall.

Hotspot WAN Metrics

The information based on WAN link connection availability through the WLAN is provided by this element to UE (Wi-Fi Alliance 2012) (Rukus 2013b). The parameters shown in Table 9 are required to be configured by the hotspot operator to provide information about the egress interface from AP to Internet if egress interface is not embedded in the AP. Otherwise, AP provides some or the all information related to WAN metrics.

Table 10. WAN Metrics.

Parameter	Setting options
Link status	Link up Link down Link in test state
WAN link symmetry (whether link speed is the same in the uplink and downlink)	Symmetric Asymmetric
Downlink speed	Nominal, in kilobits/s
Uplink speed	Nominal, in kilobits/s

Apart from the parameters seen in Table Xx. AP might additional information that could be implementation based;

• Downlink load

• Uplink load

• At capacity: If AP is at its capacity no more users will be associated to the AP.

• Load measurement duration (LMD): This parameter indicates the time interval over which the DL and UL is measured. This load measurement duration parameter is recommended to be from 1 to 15 minutes.

For UE to select the AP that can answer to its throughput requirements, WAN metrics is an extremely useful element in taking network selection decisions.

Hotspot Connection Capability

The availability of commonly used communication IP protocols (TCP, UDP, IPsec) and ports (21, 80, 443, 5060) is provided by this element (Rukus 2013b). Only certain communication protocols and ports might be available via a firewall upstream of an AP as the hotspot operator may configure the AP with the information according to protocol and port number values by setting its value as open, closed or unknown (Wi-Fi Alliance 2012).

By the information provided in this element, UEs use it to perform network selection decision according to the services supported at the AP such as HTTP/HTTPS, VPN protocols, FTP, ICMP, or others (Rukus 2013b). For example, IP value 6 and port number 443 is required by an UE running a TLS VPN application. In such a case if traffic through port 443 is not allowed then UE will not connect to the AP. One other example, "A mobile device using an Internet Protocol Security (IPsec) VPN (with or without User Datagram Protocol [UDP] encapsulation) requires the protocol/port values 17, 500; 17, 4500; and 50, 0 all to be open at the hotspot. If this is not the case, the device will not associate to the AP if availability IPsec VPN is required." (Wi-Fi Alliance 2012).

Operating Class Indication

The operating class indication element provides information based on the used channels and frequency bands by the AP in the hotspot. Hotspot operator may provide additional information indicating the operating classes that are used by other APs having the same SSID in a specific venue in case of a hotspot with multiple APs.

Due to the information provided through this element, UE may want to associate with an AP that supports frequency band at 5 GHz in case if it is preferred frequency band and if it is available through that AP.

Network Authentication Type Information

When ASRA is set to 1 this element provides information that contains a list of network authentication types (Figure 30) (IEEE 802.11u 2011).

	Info ID	Length	Network Authentication Type Unit #1 (optional)	Network Authentication Type Unit #2 (optional)	…	Network Authentication Type Unit #N (optional)
Octets:	2	2	variable	variable	…	variable

Figure 30. Network Authentication Type Information format (IEEE 802.11u 2011).

The value of the network authentication type indicator that is the subfield of network authentication type unit is chosen from Table 11.

Table 12. Network Authentication Type Indicator definitions (IEEE 802.11u 2011).

Value	Meaning
0	Acceptance of terms and conditions
1	On-line enrollment supported
2	http/https redirection
3	DNS redirection
4–255	Reserved

The value 0 means that UE needs to accept the terms and conditions of the network, redirect URL may be used by UE to obtain this information. The value 1 stands for the online enrollment and it may expect the UE to create an account and redirect URL is set to 0. The value 2 indicates that network infrastructure provides http/https redirection, redirect URL is in use by UE to function additional steps for network access. The value 3 informs UE of the DNS support by the network. Redirect URL is set to 0.

3.2.4 Capability Query ANQP Elements

Hotspot Query List

UE queries an ANQP query list with info ID of each required ANQP element in ANQP query ID fields via GAS request to APs to simultaneously obtain information in a GAS response based on the elements added in to this list. In response the AP informs the UE about how the elements are configured by the hotspot operator. The format of the ANQP Capability list is provided in Figure 31.

	Info ID	Length	ANQP Query ID #1	ANQP Query ID #2 (optional)	…	ANQP Query ID #N (optional)
Octets:	2	2	2	0 or 2	…	0 or 2

Figure 31. Hotspot query list format (IEEE 802.11u 2011).

Hotspot Capability List

Based on the hotspot ANQP query list AP transmits hotspot capability ANQP list to UE in a GAS query response. This element indicates the capabilities that are configured in AP by the hotspot operator (Figure 32).

	Info ID	Length	ANQP Capability #1	ANQP Capability #2 (optional)	…	ANQP Capability #N (optional)	ANQP Vendor-Specific list #1 (optional)	…	ANQP Vendor-Specific list #N (optional)
Octets:	2	2	2	0 or 2	…	0 or 2	variable	…	variable

Figure 32. Hotspot capability list format (IEEE 802.11u 2011).

The info IDs that are indicated in the hotspot query list will return the requested ANQP element in the query response list with a non-decreasing info ID value. Info IDs are not repeated except for the ANQP vendor-specific list. The presence of the ANQP vendor-specific list element stands for the capabilities of the vendor-specific query protocol.

NAI Home Realm Query

UE sends NAI home realm query by providing the NAI realms for which it has authentication credentials to APs. AP compares these realms with the realms whose networks or services are accessible at the AP and accordingly informs UE whether it can authenticate the UE or not by responding to UE with a list of realms that exactly match the names in the NAI home realm query list.

4. SECURE AUTHENTICATION AND CONNECTIVITY

The communication link held through the air is much more critical in terms of security considerations compared to the communication link held through cables (Nakhjiri M., Nakhjiri M. 2005). Therefore, security has a high importance of WLAN communication as the communication medium between UE and AP is air. This chapter concentrates on secure authentication and connectivity that provide a cellular like functionality. First, general information about the evolution of WLAN security is given. Subsequently, WPA2-Eterprise security is studied in details followed by some other security considerations. Finally, EAP-TTLS/MSCHAPv2 authentication based scenarios are provided in terms of home and visited WLAN.

4.1 Security Features and Hotspot Network

WFA hotspot 2.0 specification provides ease in access to WLANs in discovering and selecting a SP. When the selection of the Hotspot is completed the UE performs the authentication and connection processes which lead the connection to Internet or other networks. Although the authentication and connection are out of the scope of the Passpoint specifications they are must to be implemented by HOs and SPs. (Aruba Networks, Inc. 2011).

4.1.1 Evolution of Wi-Fi Security

WFA has put a high effort on security since the program has launched in 2000. The first introduced security solution was WEP; however, while the IEEE 802.11i was being developed WFA introduced WPA in 2003 as a short-term stronger security solution to meet market demand. Later on, as IEEE 802.11i is ratified in 2004 WFA introduced WPA2. (Wi-Fi Alliance 2012b).

As a security mechanism, WEP was introduced to fulfill security needs that are equivalent to wired networks; however, WEP was weak due to short key length (40bits in original standard but nonstandard extensions support up to 256bit) and it was devoid of reply detection (Sukhija S., Gupta S. 2012). Therefore, UE had to strengthen WEB with VPNs or 802.1X to achieve their security requirements (Wi-Fi Alliance 2012b).

To address the flaws of WEP, WFA brought WPA in to the market without requiring new hardware. WPA may be mainly considered as the subset implementation of the IEEE 802.11i amendment features and the solution for the cryptographic problems of WEP. TKIP is used for data encryption and IEEE 802.1X is used for authentication in WPA. (Wi-Fi Alliance 2012b).

WPA2 is an enhancement of WPA and a complete implementation of IEEE 802.11i standard. Although, it was introduced in 2004 as an optional certification it became a mandatory requirement in 2006 for the certification of the new equipment. By including CCMP protocol with the AES block cipher, WPA2 introduced a stronger encryption and became the most widely trusted security framework. (Wi-Fi Alliance 2012b).

4.2 WPA2-Enterprise Security

The WPA2 that is also known as IEEE 802.11i is a replacement for the previous security mechanisms such as WEP and WPA. CCMP that provides data integrity and confidentiality is a specific mode of AES used in WPA2. AES is accepted to be more secure compared to RC4 stream cipher which is used by WEB and WPA.

There are two main phases of WPA2, authentication and encryption, highly required for a secure WLAN. The encryption phase requires AES but also covers TKIP for the backward compatibility with existing hardware. The authentication phase is considered separately for personal and enterprise use. While the usage of PSK is required for personal use, the IEEE 802.1X authentication standard is used for enterprise mode. (Arana P. 2006).

An authentication server is not required for the personal mode in WPA2. Authentication is only performed between UE and AP by generating a plain-text pass phrase from 8 to 63 characters that is 256 bit PSK. PSK, SSID and the length of SSID is used later for the key generation.

Unlike in personal mode, AP functions as the authenticator by providing access control and authorization decisions are made by the authentication server (RADIUS) in enterprise mode. UE and AP communication is held over Layer 2 EAPoL. Before AP forwards the EAPoL messages to RADIUS it converts them to RADIUS messages. RADIUS that is compatible with UE's EAP types process the authentication request. Once the authentication request is successfully done UE and AP have a secret MK. (Arana P. 2006).

There are few implementation requirements in case of hardware/software in enterprise mode, stated as fallowing. The selection of EAP types are required to be performed on APs and authentication servers deployment of RADIUS based authentication servers and WPA2 software upgrades for APs and UEs.

4.2.1 Mutual Authentication

To avoid UE from connecting to a rogue network mutual authentication is performed (Wi-Fi Alliance 2012a). Based on the IEEE 802.1X authentication standard, UEs are separately authenticated in the enterprise mode by using EAP standards. In WFA Hotspot 2.0 specification, there are four EAP standards to be chosen by UE which are EAP-TLS, EAP-TTLS, EAP-SIM and EAP-AKA (Rukus 2013b). It is not possible for Passpoint APs to be arranged for P2P, DLS, TDLS, TKIP or WEP (Wi-Fi Alliance 2012a).

While the UEs with SIM or USIM are required to support all the mentioned EAP methods, UEs without SIM or USIM do not necessarily need to support EAP-SIM or EAP-AKA. An AP is required to support at least EAP-TLS or EAP-TTLS, or both. If the hotspot operator wants to provide service to SIM/USIM users or has a SIM/USIM infrastructure it is required to provide support for EAP-SIM and EAP-USIM. By these

obligations it is aimed to ensure authentication for UE with one of the EAP methods. (Wi-Fi Alliance 2012a).

Table 13. Credential Types and EAP Methods.

Credential Type	EAP Method
Certificate	EAP-TLS
SIM	EAP-SIM
USIM	EAP-AKA
Username/password (with server-side certificates)	EAP-TTLS with MS-CHAPv2

There are four phases established for a secure communication in WPA2. In the first phase, UE and AP agree on a security policy. This information is sent in the RSN field in the beacon and probe response frames containing authentication methods (802.1X, PSK), security protocols for unicast and multicast traffic (CCMP, TKIP etc.) and support indication for pre-authentication for seamless handover. (Figure 33) (Lehembre G 2005).

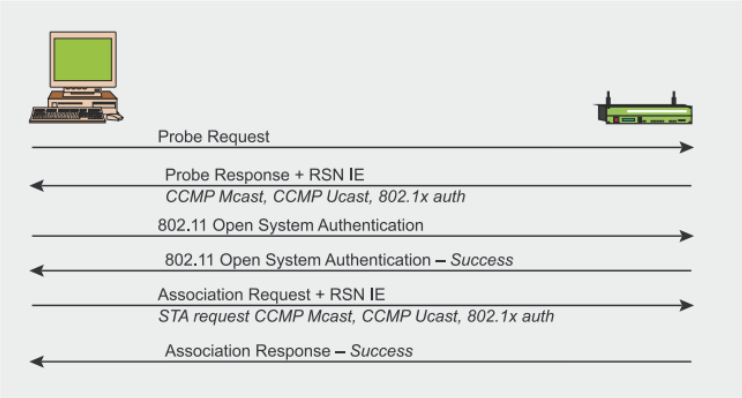

Figure 33. UE and AP agree on a security policy.

The second phase stands for the 802.1X authentication based on EAP methods to generate a common master key. The authentication is initiated by the AP requesting the client identity information from UE (the preferred EAP method). UE provides the preferred EAP method to AP and AP performs a query to authentication server for RADIUS access. Subsequently, EAP messages are exchanged between UE and

authentication server to generate a common MK. At the final stage RADIUS accept message is sent to AP to inform UE of the MK and EAP success message. (Figure 34) (Lehembre G 2005).

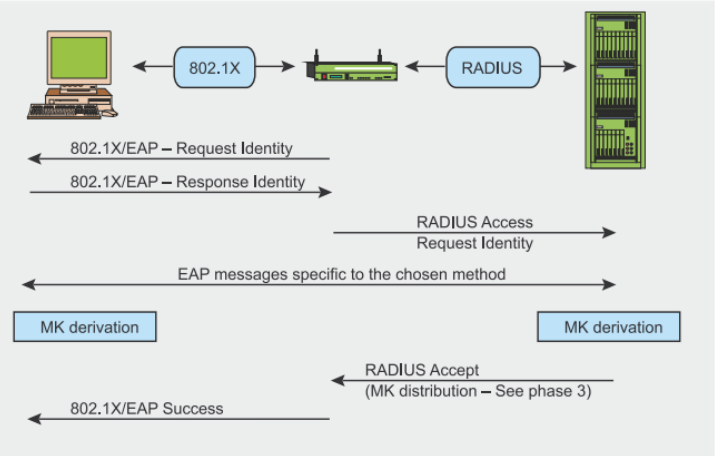

Figure 34. 802.1X authentication based on EAP methods.

In the third phase, session keys are created and updated regularly; the aim is to provide key generation and exchange. During the generation two handshakes occurs; 4-Way Handshake for PTK (Pair-wise Transient Key) and GTK (Group Transient Key) derivation and Group Key Handshake for GTK renewal. (Figure 35)

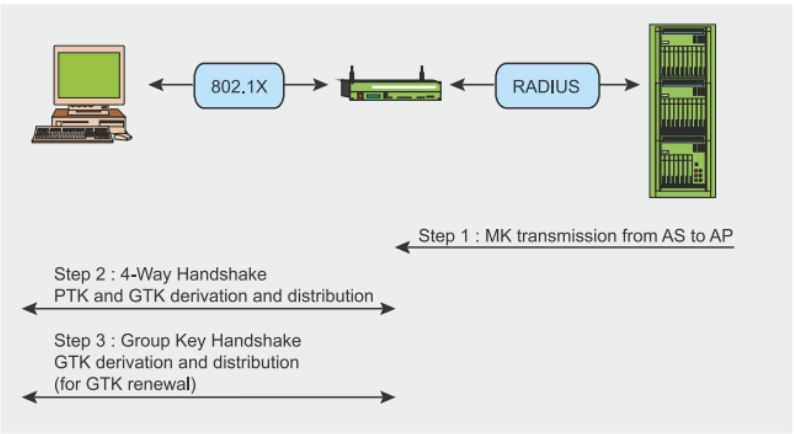

Figure 35. Session keys.

The fourth phase is about the usage of the previously created keys by the CCMP protocol for data integrity and confidentiality.

4.2.2 Advanced Encryption Standard

Air link encryption is required in WPA2 by using 802.11i. WFA Hotspot 2.0 specification provides AES technology with 802.11i that is used in wireless communication between UE and AP. Due to this implementation the security level is increased as it is in cellular service. (Rukus 2013b).

It is the first encryption standard that is openly available and protects sensitive and classified information. The data flow, in WPA2 network, is encrypted by using CCMP algorithm with AES; together they provide the most secure encryption method. In enterprise networks, AES support is highly required universally by many protocols and applications.

AES is considered to be one of the most secure encryption algorithms in the market. For an attacker it is enormously difficult to figure out the keys to eavesdrop on the communication between UE and APs. Besides, AES provides integrity protection that makes it impossible for an attacker to do a man-in-the-middle attack. The encryption keys of AES (PTK and GTK) are derived from the matchless PMKs that are created from 802.1X authentication process. (Wi-Fi Alliance 2012).

4.2.3 WPA2 Short Comings

WPA2 is expected to be the strongest security feature for wireless networks so far; however, this does not imply that it is impossible to break it. Weaknesses and disadvantages of WPA2 may be counted as follows. (Arana P. 2006) (Sukhija et al. 2012).

- Denial of Service (DoS) attacks like Layer 2 session hijacking, jamming and data flooding are all against availability. As all the Wi-Fi security standards operate on Layer 2 and above they cannot prevent attacks on the physical layer. Besides control frames like Request to Send (RTS) and Clear to Send (CTS) are not encrypted and this makes them prone to DoS attacks.

- As GTK is shared among all the authorized UEs of the network a malicious authorized client may transmit spoofed GTK packets in the network. Therefore, an authorized user can decrypt data of other UE and may install malware and compromise other UEs that is known as Hole196 attack. Port-based 802.1X access control protocol based WPA/WPA2 Enterprise is prone to this attack type.
- De-authentication, here the attacker aims to force the UE to re-authenticate. As there is no authentication for control frames that are used for authentication and association it is probable for the attacker to spoof MAC addresses.
- Disassociation: An authenticated UE is forced by an attacker with multiple APs to disassociate from them. By this way the forwarding of packets to and from the user is affected.
- WPA2 is considered to be expensive for the already deployed networks as the implementation of CCMP and AES requires change in the existing network hardware.

4.3 Authentication Methods

4.3.1 EAP-TLS

EAP-TLS that performs TLS handshake for the authentication process is based on digital certificate exchange between UE and the authentication server. It is a well-documented, extensively analyzed authentication protocol and has no significant weaknesses in the protocol. Therefore, it attracts many in case of security-related use.

Basically, first the authentication server presents a certificate to the UE. Right after the validation of the certificate by UE, based on the implementation, a certificate by UE is provided to server by a protection of a passphrase or PIN.

However, dealing with certificates is time consumption and cumbersome administrative work. In case of losing the access to the network certificates must be revoked which is

not a desired situation. The most important one is that EAP-TLS do not protect the user identity but only the user's authentication material. As a result, EAP-TLS is found to be secure; however, the UE side certificate requirement makes TTLS and PEAP more attractive methods to be implemented.

In case of using TLS as an authentication method it is used as EAP-TLS that uses digital certificates at both UE and authentication server sides. Digital certificates are known to be a very secure authentication method; however, the way of generating and distributing the certificates may be complex. Therefore, operators mainly avoid using EAP-TLS authentication method.

4.3.2 Tunneled Authentication

TLS that is based on secure socket layer plays a vital role in wireless network security as its objective is to establish a highly secure encrypted and authenticated channel to protect data flow over links that might be a subject to eavesdropping. This security may be observed in two ways: firstly it may be used as an authentication protocol by using UE and server side certificates (EAP-TLS), and secondly, it may be used to provide a secure tunnel for other authentication protocols transmission such as EAP-TTLS or PEAP.

As it has been stated, TLS may be used to protect legacy authentication protocols in a two-step protocol which could be called as outer and inner. In the first step, the outer step, a tunnel is established by TLS identifying the authentication server to the UE using a digital certificate. By this way a secure tunnel is created for the second step to perform the authentication of the UE and it provides message integrity so that no interfere occur with the authentication by an attacker. In the second step, the inner step, a legacy authentication method is used through the tunnel created in step one to deliver the UE credentials to authentication server and by doing this it provides TLS encryption so that an attacker cannot eavesdrop on the authentication.

4.3.3 Inner Authentication Methods

Password Authentication Protocol (PAP): As the user credentials are transmitted unencrypted across the network it is not desired to be used over a network that does not provide privacy protection. It is not an EAP method and it is only used by TTLS. By its use in TTLS the user credentials are protected in TLS tunnel. It is mainly selected by the designers that wish to one-way encrypt the passwords. If the passwords are not reversibly encrypted the user prove its identity by sending the password to authentication server.

Challenge Handshake Authentication Protocol (CHAP): Like PAP, it is not an EAP method and it is only supported by TTLS. In CHAP the password is required to be in clear text at the both ends which means that CHAP is a reversibly encrypted method. It is preferred by network managers that wishing to pass the password between the client and the authentication server.

The security factors found in CHAP are not relevant to the ones in 802.1X; however, the network managers who have challenge-response authentication infrastructures will want to use CHAP in their wireless environment.

Microsoft CHAP (MS-CHAP): It was designed by Microsoft to provide enhanced functionalities for Windows systems. It is beneficial to be used in environments using Microsoft authentication databases; however, because of security issues it is only recommended to be used for very old Microsoft systems such as Windows 95/98. MS-CHAP is also not an EAP method but only supported by TTLS.

Unlike CHAP, the shared-secret is not stored at both ends of the link. Instead MS-CHAP uses one-way cryptographic hash of the password to store the password on authentication server. Due to this, a matching password can be created at both ends and then it can be used in a challenge/response handshake.

Microsoft CHAP version 2 (MS-CHAP-V2): This method was introduced to address the shortcomings of MS-CHAP by removing the weak password encryption for older clients, providing mutual authentication, and improving keying and key generation.

Unlike the previous methods, it is an EAP method except being a PPP method and can be used as an inner authentication method for both TTLS and PEAP.

EAP-MD5: In case of basic structure it is similar to CHAP. Like CHAP, it needs that the password be available at both ends. Unlike CHAP, it is an EAP method and can be used with TTLS or PEAP. However, it is not recommended to be used as an inner authentication method but in non-wireless environments outside of TTLS or PEAP.

EAP-Generic Token Card (EAP-GTC): This method may be used by itself as it does not need to be tunneled inside another authentication method like TTLS or PEAP; however, it should be used inside TTLS or PEAP to provide server authentication in the wireless environment. In case of using reusable passwords, EAP-GTC must be used as an inner authentication method. EAP-GTC is mainly preferred by network operators in case of having token cards, or as a workaround to the lack of a PAP-like authentication method within the panoply of EAP methods.

4.3.4 EAP-TTLS

EAP is a simple authentication protocol providing a framework in terms of user authentication in a network within IP networks. In EAP, authentication process is defined as a framework that points to a specific authentication protocol such as EAP-TLS and EAP-TTLS that are referred to as EAP methods. In general, such protocols performs authentication with a remote server, e.g. RADIUS. (InterDgital 2012).

EAP-TTLS is a newer method compared to EAP-TLS which is developed to overcome the drawbacks of EAP-TLS that are mentioned below.

Need for client certificate: For mutual authentication both UE and server provides certificates; however, when UE is not capable of using certificates or does not need to authenticate itself EAP-TLS has less importance to be applied as the requirement of certificate from UE might be demanding; adding the load of certificates, complexity and CRL creation process. For example, if the UE needs to get some public information from an information server UE may not need to provide authentication

User versus device certificates: In some scenarios, user may use multiple UEs or a UE might have multiple users; however, provision is not provided in EAP-TLS to make a distinction between user and device certificates.

User identity protection: Through both the EAP identity message and certificate face value EAP-TLS does not provide privacy for the user.

Protocol efficiency: Although, EAP-TLS provides seamless handover it will still cause initial delays. Certificate will require long-lasting protocol exchanges which is not desired in re-authentication after a handover.

NAS support: EAP-TLS is a two-party authentication model which is held between UE and AP. In case of extending the model to authentication server might cause security implications.

Implementation of only a server based certificate can be much less complex than an implementation of server and user/device certificates separately as the number of users/devices is much higher compared to the number of the servers. Therefore, network designers try to avoid from using certificate based authentication implementations.

In EAP-TTLS the authentication server uses a certificate to authenticate itself to UE with a TLS handshake. Subsequently, a secure TLS tunnel is established so that UE may perform authentication with server.

One other main criterion for EAP-TTLS is providing secure connections in case of roaming which requires UE to authenticate and establish pair-wise keys with AP that belongs to a network does not provide trust relationship with UE. Initially UE will not provide its authentication credentials to any untrusted APs and other entities between UE and authentication server until a secure TLS tunnel is established. EAP-TTLS method defines TTLS server to support this need. (Nakhjiri et. al. 2005).

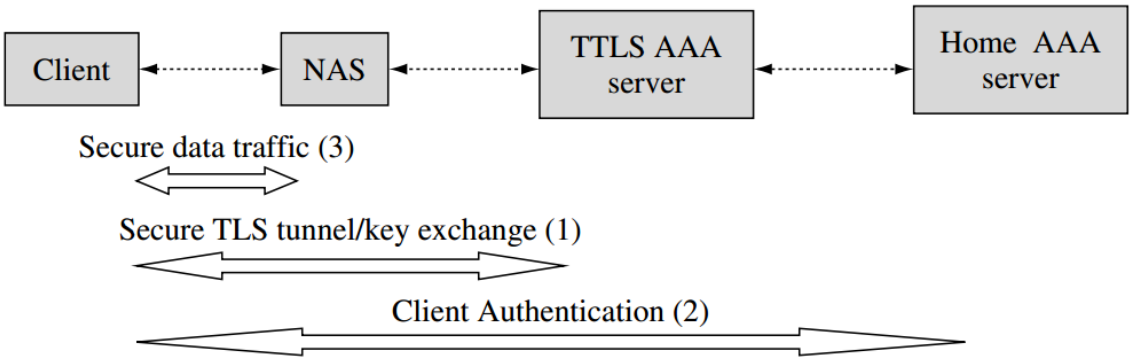

Figure 36. The interactions between the functional elements within the EAP-TTLS architecture.

TTLS server may be physically collocated at home AAA server or at NAS and there might be AAA proxy servers between TTLS server and NAS, and between TTLS server and home AAA server.

EAP-TTLS method stands for the protection of the communication between UE and TTLS server; however, the transmission of the credentials from TTLS server to AAA server must be secured as well, typically over an AAA protocol. AAA server is required to support EAP-TTLS if it is not the TTLS server at the same time; however, it is required to support legacy UE authentication mechanisms.

4.3.5 PEAP

PEAP is known to be a member of EAP family protocols. By using the TLS it establishes an encrypted channel between UE and authentication server and it encapsulates the EAP method trough this channel. It is not an authentication protocol but only increases the security level for the EAP authentication protocols such as EAP-MSCHAPv2 (Microsoft 2008).

It was jointly developed by Microsoft, Cisco and RSA security. There are three versions of PEAP, PEAPv0, PEAPv1 and PEAPv2. PEAPv0 that is referred to PEAP is the second most broadly supported EAP standard following the EAP-TLS. In PEAPv0 that uses MSCHAPv2 as the authentication method, UE provides its credentials as

password/username rather than a certificate. It is considered to be inexpensive and much easier compared to EAP-TLS or PEAP-TLS. (Weston 2008).

EAP-TTLS and PEAP are very similar in design and were designed at the same time Wi-Fi Alliance (2012c). As in EAP-TTLS, PEAP uses public key certificates for server authentication and requires PKI certificate at the server for a secure TLS tunnel to provide the protection of the user credentials. Both TTLS and PEAP have two stage protocols to establish a strong encrypted TLS tunnel in stage one and trough this tunnel exchanging authentication credentials in stage two.

AVPs that are exchanged trough TLS tunnel in TTLS provides TTLS to support nearly any type of authentication mechanisms, all EAP methods as well as some older methods such as PAP, CHAP, MS-CHAP and MS-CHAPv2; however, PEAP only supports a second EAP exchange in TLS tunnel, EAP-MS-CHAPv2, EAP-TLS and EAP-GTC (ttls and peap). This situation is considered to be the main difference between TTLS and PEAP.

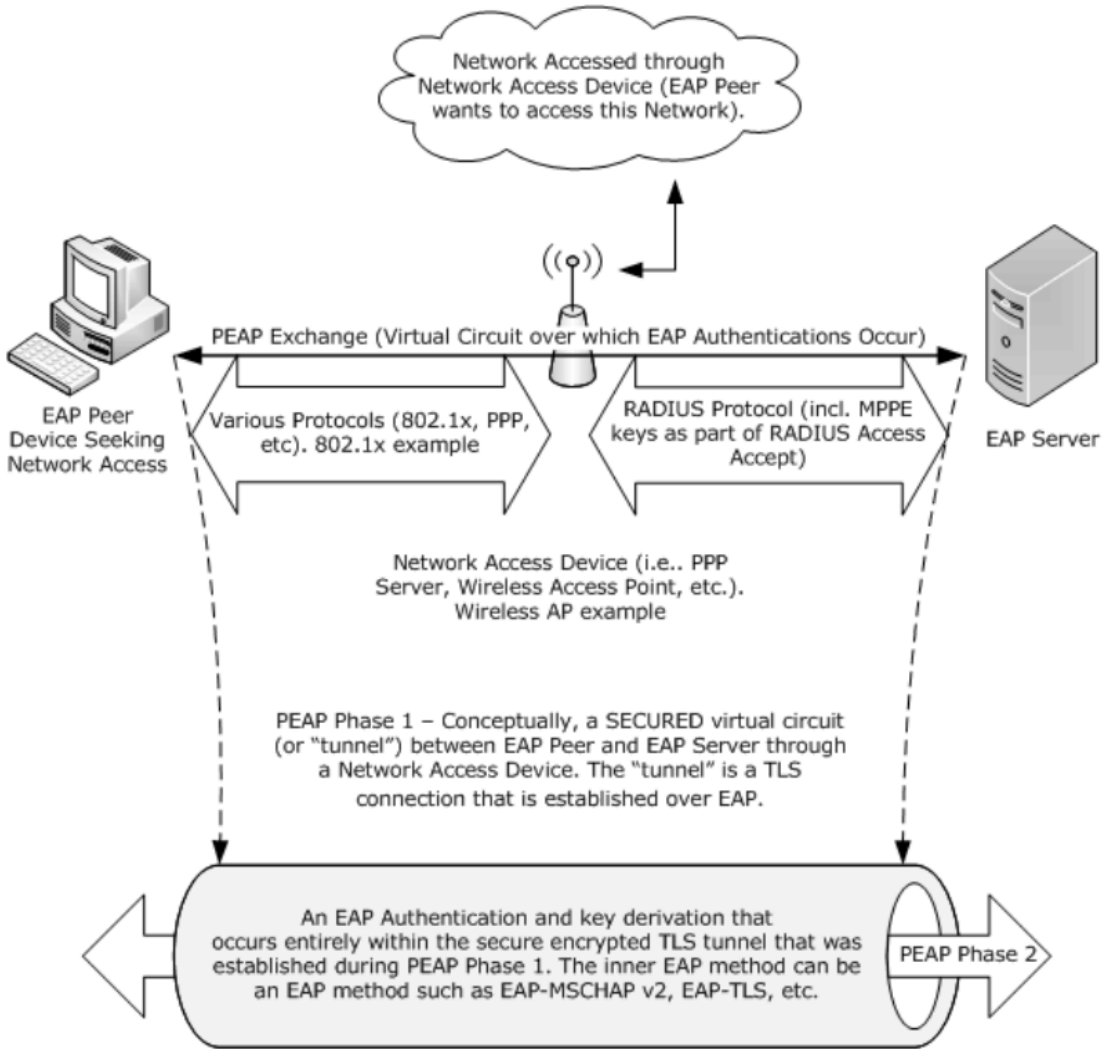

Figure 37. PEAPv0/EAP-MSCHAPv2 authentication method.

The major advantage of PEAP is the full support from Microsoft besides of being supported by IOS and Android. While EAP-TTLS is stated as one of the main authentication methods by WFA it has no support by Windows mobile devices which directs the network operators to PEAP instead. There was not a native support for EAP-TTLS/MSCHAPv2 in Windows XP, Vista and 7; however, support was being provided by Encryption Control Protocol certified software and by Windows8, Windows started to provide support for EAP-TTLS; however, no effort has been done in case of TTLS support in Windows mobile phones.

In case of only considering the authentication types but not Passpoint based on the certified product search section in WFA's official website, EAP-TTLS/MSCHAPv2 is supported by 3336 devices (including all types of devices: smartphones, access points etc.) and PEAPv0/EAP-MSCHAPv2 is supported by 4139 such devices in overall. In case of Passpoint, all the devices that are Passpoint certified support both authentication methods.

4.3.6 Other Security Considerations

L2 Traffic Inspection and Filtering

In the inspection phase of the L2 traffic, MSDUs are verified in terms of matching a specific set of traffic filters in AP or firewall which performs filtering. MSDUs are only delivered from one UE to another UE that is addressed to it. In the filtering phase, an UE is aimed to be protected from other UEs that tent to attack. In hotspot 2.0 specification, any Passpoint AP that functions as a public network is required to support L2 traffic inspection and filtering of data communication between UEs in the same BSS or ESS. (Wi-Fi Alliance 2012a).

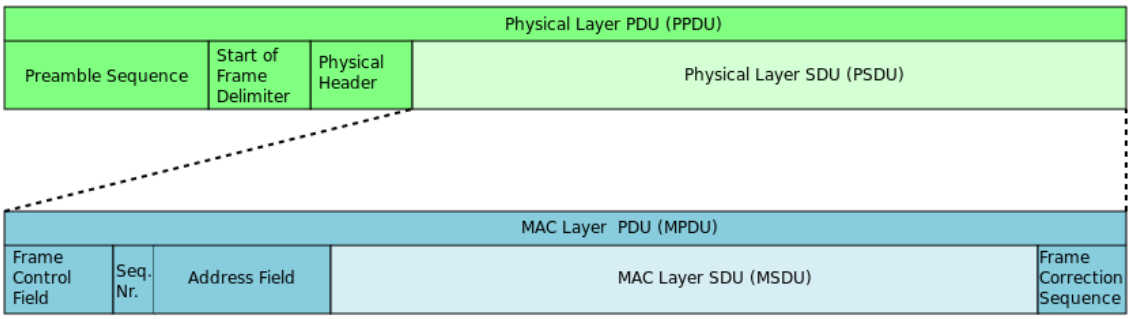

Figure 38. PPDU frame format.

A firewall that resides in an AP or in an external unit that AP is connected protects the AP and the UEs that are connected to it from attacks over internet and also it protects UEs from other UEs' attacks. Therefore, HOs must deploy firewall in their network.

Deactivation of Broadcast/Multicast Functionality

In case of disabling the multicast/broadcast functionality, GTKs are not used which means an attacker that has authenticated to the network cannot perform hole-196 attack by sending to AP spoofed packets encrypted with GTK. Therefore it is recommended by WFA to disable the multicast/broadcast functionality for Passpoint AP if they are not providing such services, IPTV services or HD streaming services. When this functionality is disabled Passpoint AP uses proxy-ARP service; however, the usage of proxy-ARP is also recommended in case of multicast/broadcast functionality is enabled. (Wi-Fi Alliance 2012a).

4.4 PEAP/MSCHAPv2 Authentication Scenario

4.4.1 Protected EAP (PEAPv0) Authentication Exchange

The authentication process might start in two ways: first the UE sends an EAPoL start packet to AP or the AP directly sends an EAP-Request/Identity packet to UE. While this does not make any changes it only stands for the initiation of the authentication process. The authentication process seen in sequence diagram in figure 39 is based on PEAP/MSCHAPv2 method and it occurs as follows;

- The supplicant (UE) sends an "EAPoL Start" packet to the authenticator (AP). Then AP responds to UE with an EAP-Request/Identity packet to receive EAP-Response/Identity packet from UE. Subsequently, AP delivers the received EAP-Response/Identity packet to RADIUS after striping the Ethernet header and encapsulating the remaining EAP frame in the RADIUS format. The RADIUS identifies the authentication method as PEAP and based on this sends an EAP-Request packet with a PEAP start message to AP to be delivered to UE. Flowingly, AP strips the authentication header and encapsulates the remaining EAP frame in the EAPoL format to be transmitted to UE.

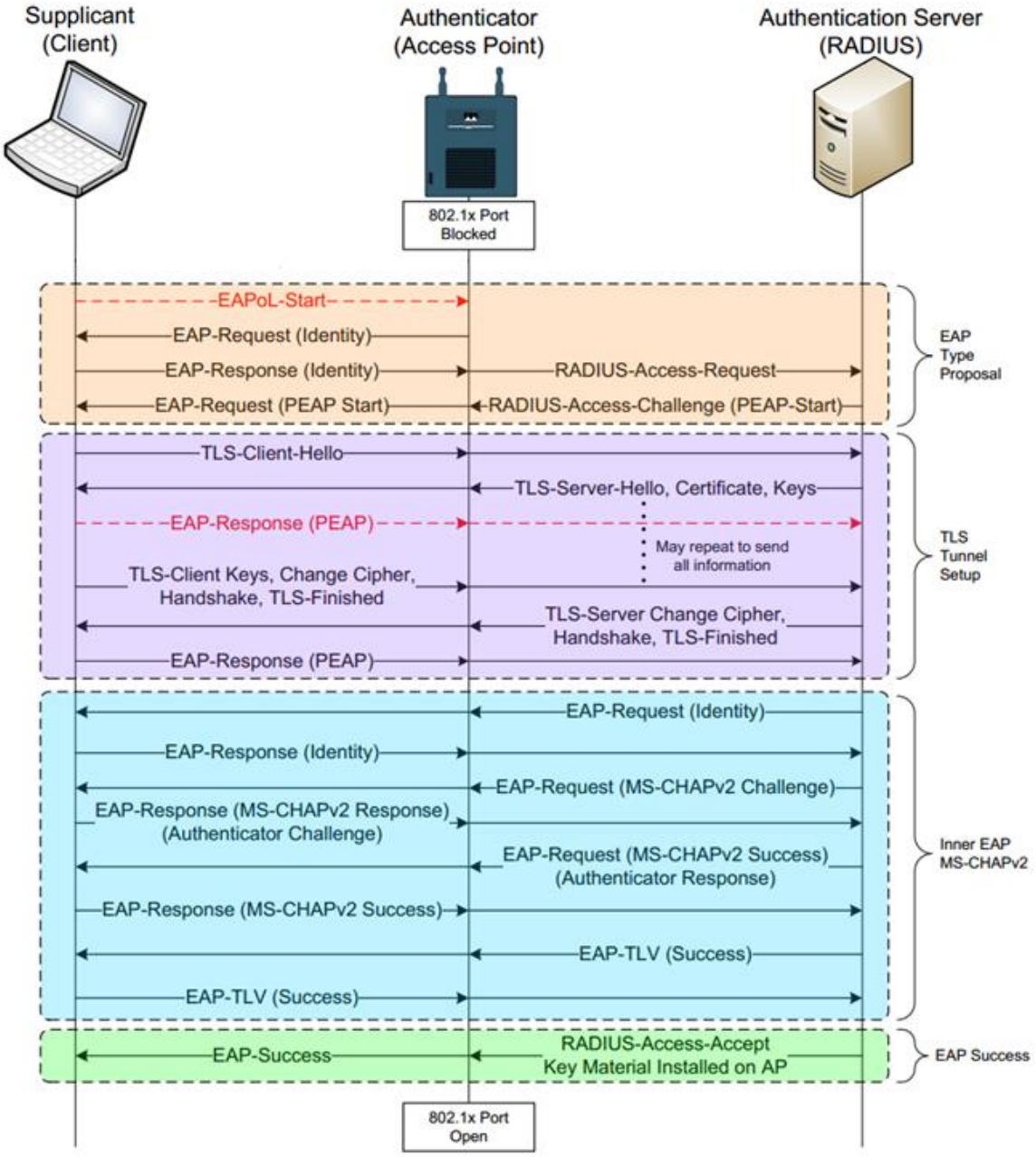

Figure 39. PEAP/MSCHAPv2 authentication sequence diagram.

- PEAP enters to step one to authenticate the authentication server to setup a TLS tunnel. UE sends an EAP-Respond packet based on TLS hello message including TLS version, a session ID, a random number and a set of chipper suites to PEAP server (RADIUS) trough AP to initiate TLS session. RADIUS

responds to UE trough AP with an EAP-Request packet that includes TLS server hello handshake message, a server certificate message and a server hello done message. Next, UE responds to RADIUS trough AP with an EAP-Respond packet including TLS change cipher spec message and a certificate verify message. Following, the RADIUS's EAP-Respond message to UE trough AP consists of TLS change cipher spec message and a finished handshake message. UE finally sends EAP-Respond packet to RADIUS to conform the establishment of the TLS tunnel.

From now on the PEAPv0/MSCHAPv2 inner authentication process is held through a secure TLS tunnel and UE identity is released through this tunnel to prevent eavesdropping.

- RADIUS sends EAP-Request/Identity packet to UE trough AP and accordingly UE responds to RADIUS through AP with EAP-Response/Identity packet. Subsequently, MSCHAPv2 challenge and success (EAP-Request and EAP-Response) packets are exchanged between RADIUS and UE, all trough AP. To indicate that UE has provided a proper identity, RADIUS sends EAP-TLV message to UE and accordingly receives back from UE an EAP-TLV status success message.

By this EAP packet exchanges UE is successfully authenticated to the RADIUS.

- As the final step, RADIUS sends an EAP-Success message to AP to indicate that AP may provide network access permissions for UE, based on this AP informs the UE with EAP-Success message.

  At this point, 802.1X port is open and the related UE has access to WLAN according to WLAN policies. However, if UE's credentials are not acceptable then RADIUS passes a reject message and AP blocks access to LAN.

5. NETWORK DEPLOYMENT FRAMEWORK

5.1 Network Core Element Requirements

By the introduction of WFA Hotspot 2.0 specification, the updates and upgrades in the hotspot operators' existing infrastructure has become an unclear issue. WFA has started the certification program for WLAN devices (e.g. access points, smartphones, tablets, notebooks) that supports WFA HS2 specification starting from 26th of June 2012 (Wi-Fi Alliance 2012d).

5.1.1 User Equipment

A Wi-Fi device that is aimed to be functioning with respect to the hotspot 2.0 specification is required to be a Passpoint certified device. Users without Passpoint certified UEs will not be able to enjoy the benefits of streamlined connectivity and secure connection at hotspots (Wi-Fi Alliance 2012d). However, the non-Passpoint UEs will still be able to associate with Passpoint certified access points that also provide open system authentication.

Passpoint UEs will be able to associate to both Passpoint and non-Passpoint APs. In case of connection with a Passpoint AP, UE will function according to the Hotspot 2.0 specification and the policy of the SP. On the other hand, UE that connects to a non-Passpoint AP functions according to the operation of the AP and the policy of the SP.

UE is expected to support the EAP authentication methods (EAP-SIM, EAP-AKA, EAP-TLS, EAP-TTLS). However, UEs without SIM or USIM do not need to support EAP-SIM or EAP-AKA respectively. Besides, UE shall support IPv6, IPv4 or both.

In case of connection policy, UE is expected to follow some attributes, such as; to allow the user to subscribe to more than one Wi-Fi CPs and perform a method to prioritize among them, to allow the user to manually select one another available open access

point at any time and to determine white and black lists of APs, to support ANQP/GAS and may support ANDSF.

Connection Manager

It is well accepted that most of the advanced features that have been introduced so far rely on the key capabilities of the UE. Connection Manager (CM) is one of these capabilities. It is the software that manages the network connections of UE, follows user and operator preferences, takes into account the network conditions etc. (InterDgital 2012).

By the implementation of the CM, Passpoint UEs may autonomously perform the Wi-Fi network selection basing on the OP policies, authenticate to the network and provide WPA2-Enterprise based link-layer security. As a result, Wi-Fi becomes to have cellular like security and mobility. Moreover, CM performs decision making to select the best Wi-Fi network when there are more than one networks available.

In terms of having ease in usage and being friendly, the user interface of the CM is considered to determine the user satisfaction regardless of the underlying standard existing in the network and phone OS or chipset (Disruptive Analysis 2011).

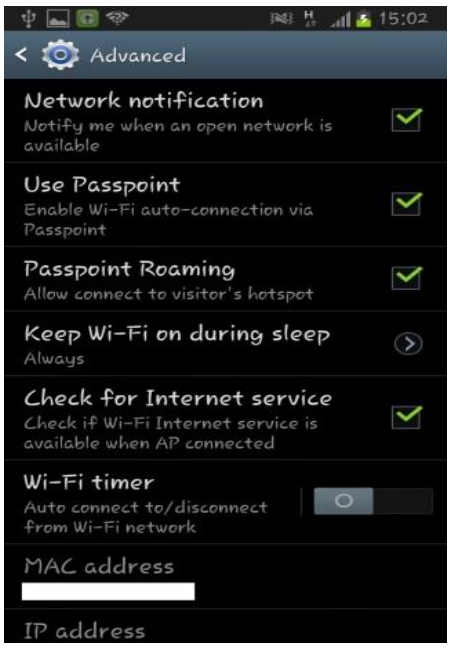

Figure 40. Samsung Galaxy SIII Advanced Wi-Fi settings.

Unfortunately, UEs do not come with a fully functional CM built in. As it might be observed from Samsung Galaxy SIII Settings -> Wi-Fi -> Advanced option, only "Use Passpoint" and "Passpoint Roaming" are available to be set, the same situation may be observed in Samsung Galaxy S4 as well. Therefore, CM may exist in the UE's OS, integrated into drivers or it may be installed as a third party SW.

IETF and Open Mobile Alliance (OMA) have started some work under the IETF Multiple Interfaces Working Group (MIF) and Connection Management Access Point Interface (OMA-CMAPI) respectively. The aim of them is to provide related functionalities to apps, users and network operators to deal with the UE's network connections successfully by considering the following criteria. (InterDgital 2012).

- taking into account the different network types,
- network discovery and selection services (e.g. ANDSF and WFA Hotspot 2.0),
- service handling,
- power management,
- contacts handling,
- security authentication and authorization such as Single Sign-On (SSO),
- location management, etc.

UE Policy

The SP policy is implemented in UE in a way that is outside the scope of the WFA Hotspot 2.0 Specification (Wi-Fi Alliance 2012a). Due to UE preferences and SP policy, UE may automatically invokes these policies and accordingly choose a preferred AP in network selection phase of the process.

Based on Passpoint Release 1, there are two basic policies are provided by Passpoint UE which are to prefer a Passpoint AP over a non-Passpoint AP and to prefer an AP that is operated by its home network operator (Rukus 2013a).

5.1.2 Access point

Replacements of existing APs with the Passpoint APs might be at a value of high cost for the operators. The technology is quite new in the market and not fully implemented. Therefore, the return of the investment might take a long run. However, being able to use the existing APs with some modifications (e.g. firmware updates) would be at a great value for hotspot operators.

Hotspot operators with existing non-Passpoint APs may be empowered to emit a second SSID that would stand for providing Passpoint functionality. Such an implementation is only possible for APs that support multiple-BSSID feature. In this case, the same radio hardware is used to transmit Passpoint SSID and to transmit the existing SSID as well. To keep the broadcast domains and networks separate and to preserve network security, these two SSIDs must be assigned to different values. If non-Passpoint APs do not provide support for multiple-BSSIDs, one another set of APs will be needed to provide Passpoint functionality. (Wi-Fi Alliance 2012a).

Some requirements that may be taken into consideration (NICC Standards Limited 2012);

- APs shall support EAP authentication methods. In addition, the support for PEAP is a plus to give service for the mobile devices that running Windows based OS.
- The number of SSIDs should be kept to minimum.
- There should be radio interfaces utilizing both the 2.4 GHz and the 5 GHz RF bands.
- AP is required to be Passpoint Certified as defined by Wi-Fi Alliance.
- At least IPv4 or IPv6 should be supported in AP. Both IP versions may be supported in AP as well.
- AP shall provide IP tunneling for example, IPSec or GRE based tunnelling.
- As the AP might not be physically secure clients' credentials should not be stored on AP.

- There should be a secure network connection provided by AP to WLC and core network.
- The control of the APs should be held via a remote management.

5.1.3 AAA Server

RADIUS is a networking protocol (server) for its remote users to provide centralized authentication, authorization and accounting services. All the user credentials might be stored in RADIUS against which the RADIUS validates user authenticity and as the configuration is not based on standards so that it can be specific, those credentials may also be stored in an exterior database, such as LDAP, SQL or Active Directory *(wifi 2005)*.

RADIUS uses UDP for message transmission, UDP port 1812 is used for authentication messages and UDP port 1813 is used for accounting messages. RADIUS messages are consist of a header and zero or some attributes such as user name, user password, IP address of the access server etc. The attributes that are carried on RADIUS messages are used to deliver information between RADIUS client, proxies and servers. RADIUS Proxy stands for the message delivery between RADIUS enabled devices (Tuladhar 2007).

RADIUS messages are defined as follows;

Access-Request: it is sent from a RADIUS client to RADIUS server to perform a connection attempt. This connection attempt is performed to request authentication and authorization.

Access-Challenge: In response to access-request it is sent by RADIUS server to RADIUS client. It is a challenge message for client.

Access-Accept: In response to access-request it is sent by RADIUS server to RADIUS client to confirm that the connection attempt is authenticated and authorized.

Access-Reject: It is also sent by RADIUS server to RADIUS client in response to access-request to inform the client that the connection attempt is rejected.

Accounting-Request: It is sent by RADIUS client to RADIUS server to agree on the accounting information for the accepted connection in previous messages.

Accounting-Response: In response to accounting-request it is sent by RADIUS server to RADIUS client. It provides information successful reception and handling of the accounting-request.

The selection of the authentication server has importance as there might be different user credential databases and matching EAP types. Operators may either change EAP types or purchase a new server to achieve a match between. However, it is recommended to change the server to match the operator's EAP types that supports their security policy in the best way.

There should be used a RADIUS proxy to forward access-request messages to RADIUS server. If RADIUS client's UE is a visitor in the network and its service provider has a roaming agreement with the visited network then the RADIUS Proxy forwards the access-request message to the Roaming Proxy and from there to UE's home RADIUS server. However, if the UE is in the coverage of its home network operator that provides service then the RADIUS Proxy forwards the access-request message to the RADIUS server that is located in UE's home network, not forwarding to Roaming proxy. For example, considering that there are two WLAN networks, ANVIA and ELISA. When ANVIA's customer is in the coverage of ELISA's hotspot, ELISA's RADIUS Proxy forwards the message to its Roaming Proxy and from there to ANVIA's RADIUS server and when it is in the coverage of ANVIA's hotspot ANVIA's RADIUS proxy directly forwards the message to ANVIA's RADIUS server.

When the UE attempts to connect to a visited network's AP the UE's home AAA Server may provide it with Home Network IP address in case if the traffic is wanted to be tunneled to Home Network. However, UE's home AAA server may also not provide it. In this case, the Visited Network provides the Wi-Fi Device with an IP address and terminates User Plane traffic to the internet. (NICC Standards Limited 2012).

5.1.4 Wireless LAN controller

A WLAN controller is a network element that is used to manage APs in large quantities by network operators. It is counted to be important to require authentication of the APs that connects to the network as there may be malicious devices trying to perform a man in the middle attack. There are some requirements for WLC in case of its implementation in WLAN (NICC Standards Limited 2012).

- As representing the APs WLC should act as a RADIUS client to RADIUS server.
- WLC is expected to redirect the new clients to a registration process or a help page.
- The propagation of the authentication storms should be prevented by WLC using an appropriate mechanism such as caching or storm control.
- The RADIUS accounting packets shall allow inter-CP cross charging and settlement in either a clearing house or a transactional model.

5.1.5 ANQP Server

WFA Hotspot 2.0 Specification is mainly based on query mechanism to/from ANQP server which is an advertisement server that is defined in IEEE 802.11u amendment and is positioned in Passpoint hotspot operator's WLAN network. The ANQP queries basically provides the Passpoint UE to discover information related to services provided in WLAN network, such as accessible roaming partners, home realms, credential types for authentication and so on. (Ellsberger 2013).

Some requirements for ANQP server;

- ANQP server is required to provide support for information query by using IEEE 802.11u amendment.
- Although, the location of the ANQP server is not indicated in the standard a logical link is required between ANQP server and WLC.

- APs need to discover ANQP server. Therefore, it is advised to place it on a centralized device that serves different APs.

When a UE performs ANQP query, the AP allocates a memory block to save some information related to query, such as the UE's MAC address, Dialog ID. Subsequently, AP transmits an internal query to ANQP server (a centralized advertisement server) that stocks ANQP information elements. (Liu Y., Li S., Xie ., Xu X. 2012).

5.1.6 Edge Router

Edge router basically connects a small network area to a wider one by providing its entries to service provider's core network. Although, the user data transmission between UE and AP is securely held the transfer of data to other network elements such as firewall or edge router also needs to be performed securely. A Hotspot 2.0 operator may establish a secure link from a Passpoint AP to a home SP core network or a roaming partner's core network. This may be achieved by restricting physical access to these devices or by using secure transport protocols such as IPsec.

5.1.7 Access Router

Access router that also known as core router is a router that forwards packets to computer hosts within a network but not between networks. It generally resides within the middle or backbone of the LAN network. In some cases, a core router interconnects the edge router from a large enterprise location (WAN).

5.2 ANVIA Passpoint WLAN Network Architecture

There are two scenarios considered in case of Passpoint network functionality. In the first scenario, ANVIA's UE is assumed to be in the coverage of the home service provider (ANVIA) that is also the Hotspot operator and accordingly the communication

between the network core elements are listed and detailed (Figure 41). In the second scenario that will be introduced right after the first one, UE is assumed to be in the coverage of a visited service provider that has an agreement with UE's home service provider to perform the authentication. In addition to these scenarios, roaming scenarios are also analyzed and presented in this section.

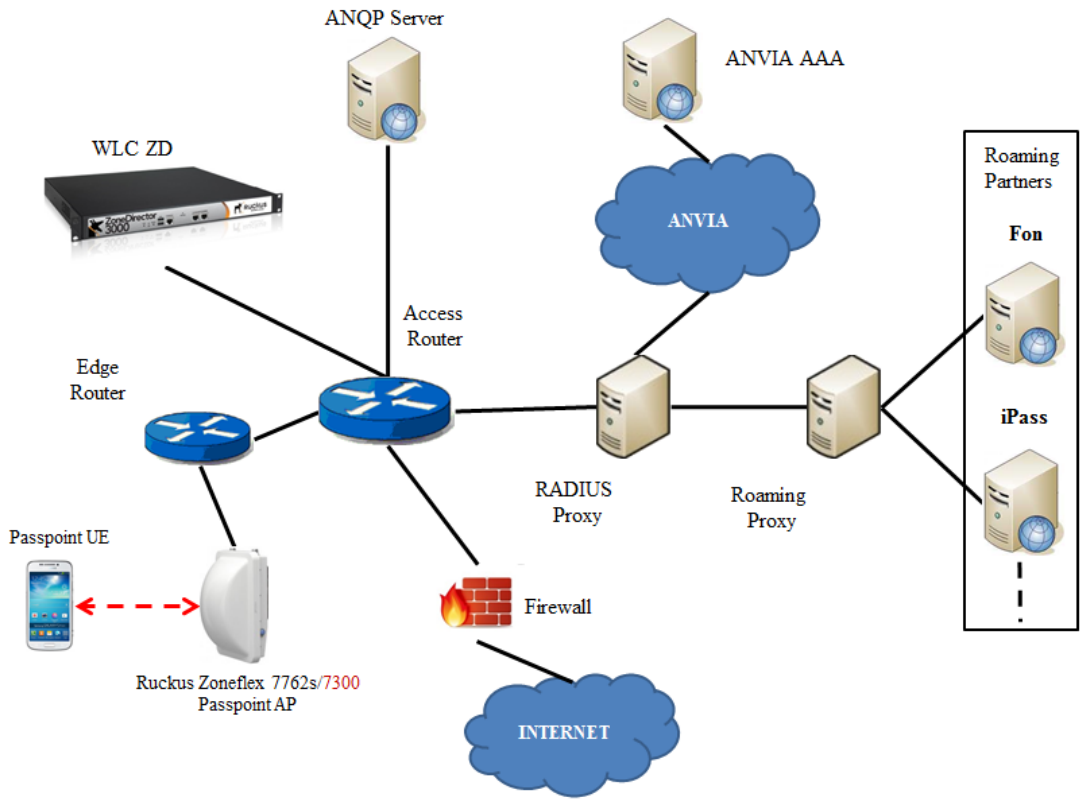

Figure 41. ANVIA Passpoint network deployment.

. A rough connection between network elements may be seen in Figure 41.

There are many minor communication steps held between some of the network core elements; however, they are not indicated in this section as they have been introduced in detail in previous chapters, such as communication between UE and ANQP Server through AP, UE and RADIUS etc.

Network discovery, selection and authentication occur as it is explained in the following steps:

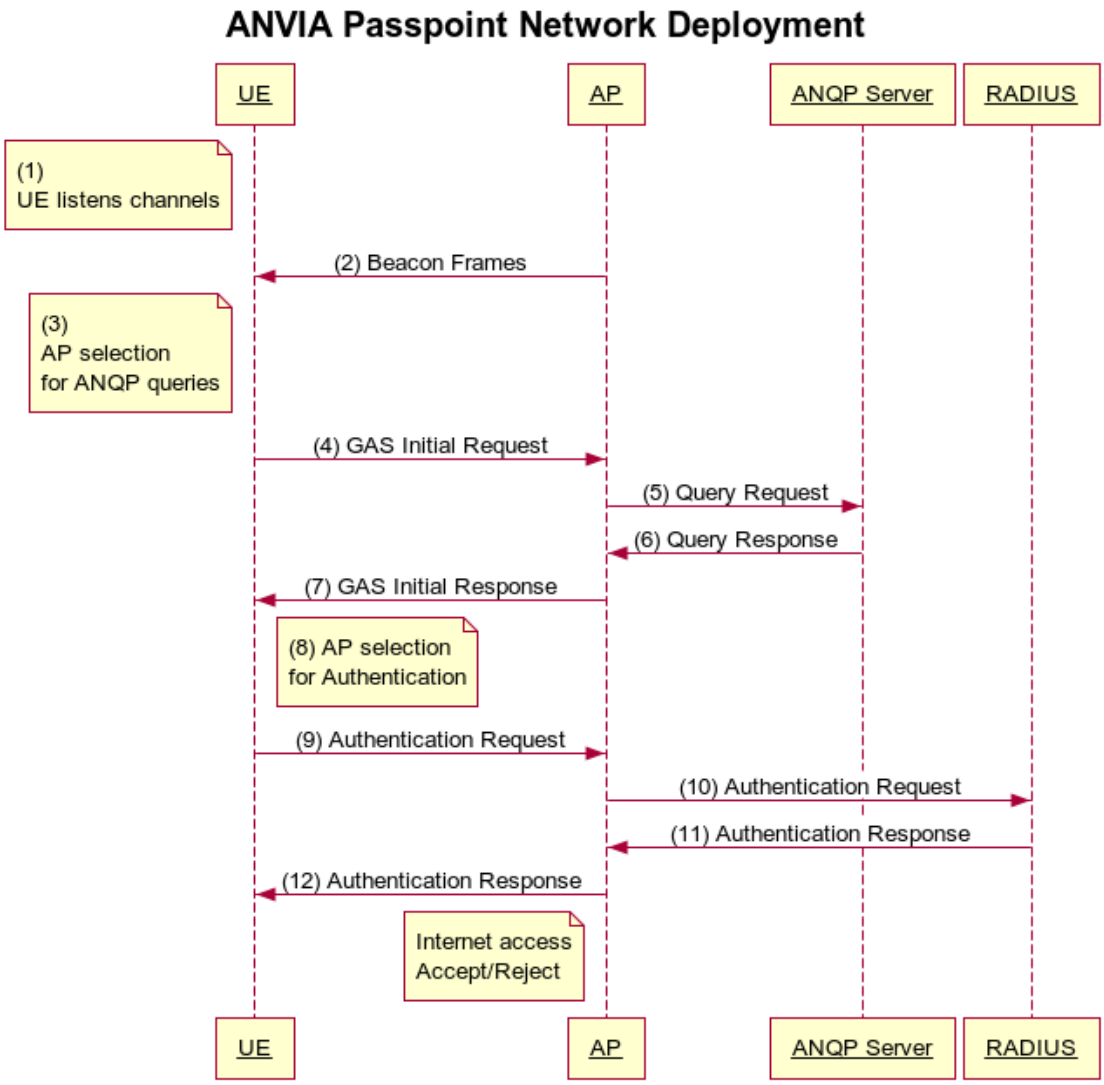

Figure 42. ANVIA Passpoint network functionality sequence diagram.

(1) UE listens channels to check whether there are any Passpoint capable APs emitting beacon frames.

As it has been explained in details beacon frames stands for basic necessary information delivery to Passpoint UEs. At this stage UE may simultaneously listen beacon frames from different APs which are in the range.

(2) Passpoint capable AP emits beacon frames.

Passpoint APs broadcast beacon frames in every 100 ms to inform Passpoint UEs that are in their coverage area about the WFA Hotspot 2.0 Specification service availability and other information frames that are explained in network discovery and selection chapter.

(3) AP selection for ANQP queries.

Based on the information gained in Beacon frames from AP(s), the CM in UE makes the decision whether to continue to perform ANQP queries. Here the policy introduced to CM plays a vital role in performing this decision. For instance if UE is not preferred to be connected to an AP that supports only IPv4 but not IPv6 then UE will not consider that AP for further process (ANQP queries).

(4) UE performs ANQP query to AP(s), or to ANQP Server directly (It is implementation depended; however, it is preferred to make ANQP queries trough AP).

If there are more than one Passpoint capable APs that are in coverage area and suitable for further process due to EU/SP policy, UE attempts to gain more information through the ANQP queries from those suitable APs as the information provided in beacon frames is limited compared to the information provided in ANQP queries.

(5) AP delivers the query request from UE to ANQP server.

AP mainly acts as a message delivery unit between UE and ANQP Server to deliver the requests and responses accordingly.

(6) ANQP Server performs the query response to AP.

In response to the required information asked in a query request, ANQP Server delivers the information related to the services available through the AP.

(7) AP delivers the ANQP query information sent from ANQP Server to UE.

If the information requested is not larger than 1 MMPDU, AP directly hands over the ANQP response to UE. However, when the requested information is large, GAS fragmentation is used to deliver the ANQP response. One other issue is that the response from ANQP Server may take a longer time than usual. In this case AP informs the UE to come back later to achieve the requested information. This step is explained in detail in second chapter, Background, under the GAS subtitle.

(8) AP selection for Authentication

So far up to this step UE\CM was being introduced about the services available through the AP(s). After the ANQP queries performed, UE\CM decides on the most suitable AP that also obeys the CM policy requirements. Although, UE may perform ANQP queries to multiple APs simultaneously only one AP chosen for the authentication process.

In the following four steps (9-12), the authentication process is performed. Although, there are many minor steps at the authentication process they are not indicated here to avoid repetition; however, for the detailed process the related sections in the 4th chapter may be read trough.

At the authentication phase, AP has no functionality but only the change the message formats. When a message comes from UE, AP strips the Ethernet header and encapsulating the remaining EAP frame in the RADIUS format with no luck of seeing the content of the message and vice versa.

In case if the UE is ANVIA's own client then the authentication credentials are confirmed in ANVIA's RADIUS server through the RADIUS Proxy; however, if the UE is belong to the roaming partner of ANVIA then the authentication request is forwarded to roaming proxy from RADIUS proxy. Roaming proxy then delivers this authentication request to the appropriate roaming partner of ANVIA.

(9) UE performs Authentication request to AP
(10) AP to RADIUS
(11) RADIUS to AP
(12) AP to UE

Until authentication phase of the connection, network discovery and selection phases are completed and subsequently authentication phase is attempted to be performed. However, if the UE has no valid credentials or if it is the first time of the connection user will be directed to a captive portal to perform the registration for the WFA Hotspot 2.0 Specification service.

Here, it is aimed to assign a username and password to UE trough captive portal. Such an implementation gives advantage to SP to provide registration for new clients to enjoy WFA Hotspot 2.0 Specification. By the registration of the UE to SP's user database, the username and the password are saved to the CM in UE so that the subsequent authentications to the network are performed automatically between UE/CM and RADIUS.

The process described above points to passive type network discovery and selection as the UE performs the ANQP queries based on the information gained in beacon frames. However, when a specific network type preference is set in CM, UE performs probe request to APs in its coverage area and accordingly receives probe responses whether such a service available or not. Based on this UE performs ANQP queries in case if it finds a suitable AP(s) to get more information and the rest of the process is same as in passive scanning.

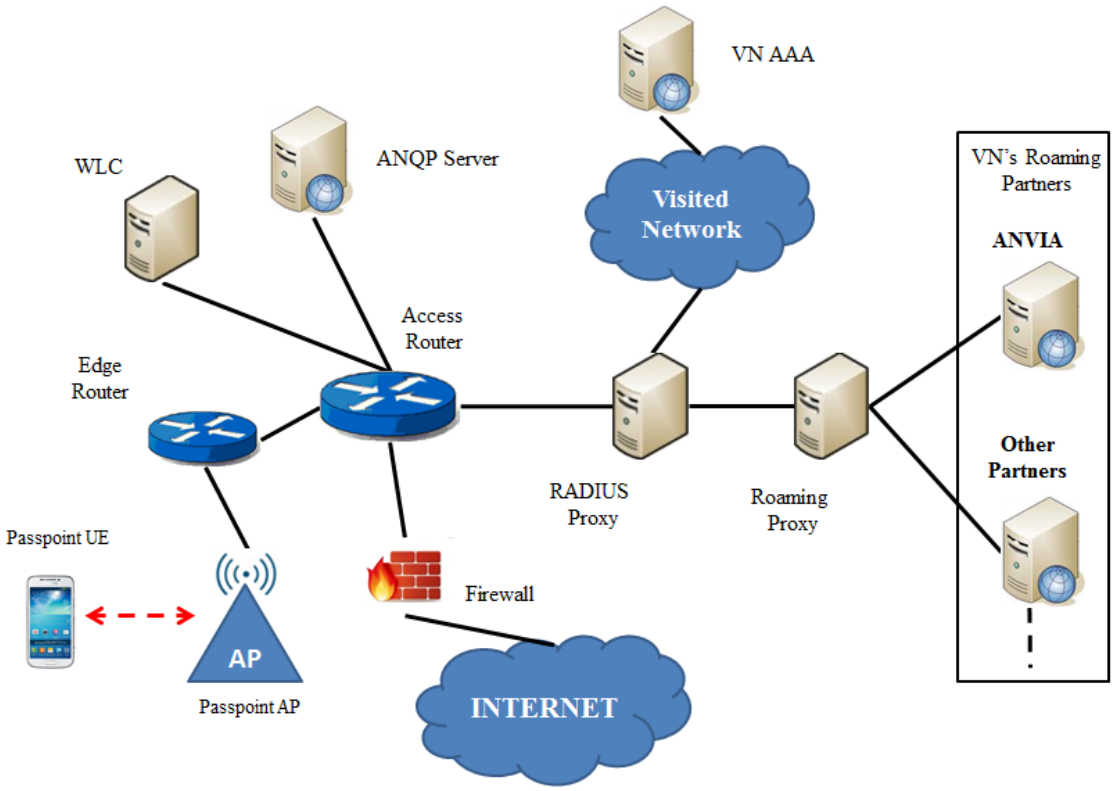

Figure 43. Visited Network Passpoint network deployment.

A similar network discovery, selection and authentication process is also performed in case of UE being in a VN coverage area (Figure 43) as the network elements are considered to be more or less similar. Here, ANVIA is assumed to be one of the roaming partners of the visited network and based on this if the UE is ANVIA's own client then the authentication will be performed between UE and the ANVIA's RADIUS server as the authentication request will be directed from RADIUS proxy to roaming proxy and from there to ANVIA's RADIUS server.

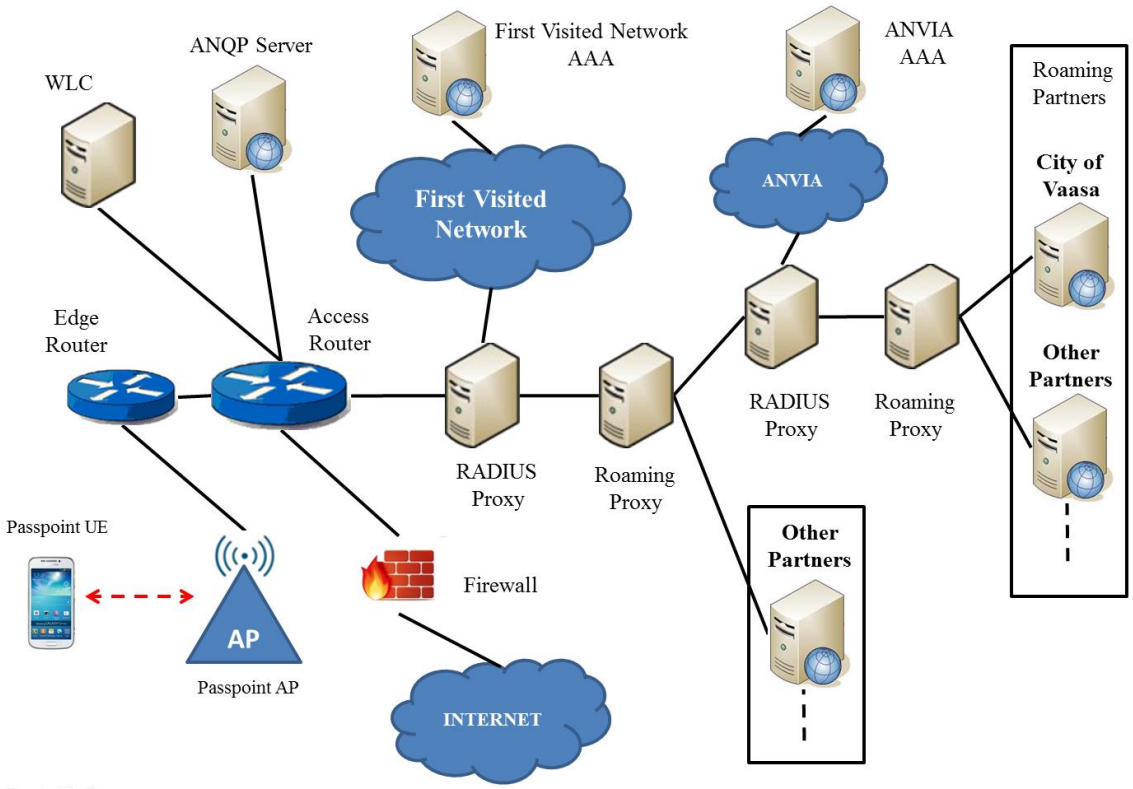

Figure 44. ANVIA inter-SSP roaming scenario.

There are some community WLAN providers such as City of Vaasa, Langaton Tampere etc. that have their own network infrastructures. As they are providing service in small local areas they might not be recognized in global market as a roaming partner in terms of providing Hotspot 2.0 Specification service to their users. However, it is considered to be the best option for those local communities to be a partner of a larger organization that would represent them in the global market.

6. PASSPOINT FUNCTIONALITY TEST

This chapter of the thesis contains confidential information and removed.

7. CONCLUSION

Due to technological developments in mobile communication devices, clients' affection to switch their UEs to the advanced ones and Internet services in large Mbps that require high data transmission such as Web browsing, streaming video and social networking have become an enormous problem for the cellular mobile communication service providers. Although, there are next generation cellular networks such as 3G and 4G the response to the expected data transmission rates cannot be achieved via cellular networks and it is considered to be a bigger problem for the future case. Wi-Fi is considered to be an excellent choice for such a requirement by having upwards of 600 Mbps data rates, being available on all the mobile communication devices and being available in all common venues; however, the challenging process of initiating a new connection to an AP and navigating between different APs from the same or different networks requires too much user intervention and valid user credentials each time as the SSIDs and the required credentials are expected to be different for each AP.

To extend the capabilities of the former Wi-Fi for enhancing the mobility experience in terms of having a cellular-like implementation, IEEE 802.11u amendment is introduced to IEEE 802.11 standards family by IEEE. Based on this new amendment WFA has also introduced some extra capabilities to it and commercialize it as WFA Hotspot 2.0 Specification. WFA is responsible for the certification of the Wi-Fi devices under the Passpoint certification program to provide a global coherence among the Wi-Fi devices. WFA Hotspot 2.0 Specification simply provides identification, selection and association to Passpoint capable APs, globally, in a highly secure manner and without any user intervention.

A wide Wi-Fi network infrastructure is available in most common areas in all around the world by many different network operators. The implementation of WFA Hotspot 2.0 Specification is going to provide not only off-loading for cellular mobile network operators but most importantly it will provide a cellular based internet connectivity for non-SIM based mobile devices that do not rely on existing cellular networks such as GSM and 3G. By this way, ANVIA is considered to gain in terms of fulfilling the customer demands; mobile, cost effective high data transmission.

In this thesis work, WFA Hotspot 2.0 Specification based Wi-Fi network discovery, selection, secure authentication and network element requirements are studied to have a great understanding of the whole system functionality. Based on these studies and discussions with telecommunication experts, network deployment frameworks and testing phases are performed in terms of different scenarios.

As this new technology recently got into the market it was not an easy task to find reliable sources to conduct this research. However, IEEE 802.11u standard, Internet sources and white papers published by different companies/organizations are used to achieve a strong background. Moreover, being in discussions with telecommunication experts inside and outside of the company has made this master's thesis to achieve its goals.

The goals that have been mentioned in research areas are successfully studied and provided in details;

- To have a good understanding of the overall system functionality, the complete communication flow between UE and Passpoint WLAN including used protocols/methods and transmission/reception frames are described and functionality tests are performed.
- Information based on Passpoint roaming to other WLANs is provided and functionality test is performed between ANVIA and Langaton Tampere WLANs due to roaming proxy configurations between authentication servers at both ends.
- Username/password based authentication process is described and tested in testing scenarios.
- Passpoint network deployment frameworks with core element requirements have been proposed and partially implemented in testing phase.

Although, information based on WFA Hotspot 2.0 Specification is limited based on CM and network deployment this thesis work has accomplished its goals. However, it is highly recommended to extent the research in terms of few areas as described in following. CM implementation has a high importance as it will provide users a manual

control of network selection. ANQP server is generally available in WLAN controllers; however, WLAN controllers are not used to manage home users' CPEs. Therefore, the implementation of an independent ANQP server may provide network operators to extend their Passpoint WLAN services to their subscribers trough home users' CPEs which means a very wide Passpoint connection availability for the Passpoint UEs. Last but not least, SIM based Passpoint connectivity is considered to be gainful in terms of providing offloading services for cellular mobile operators. The importance of such research areas is well understood and it is going to be the next step to be taken as the future work for this master's thesis.

REFERANCES

Arana P. (2006). Benefits and Vulnerabilities of Wi-Fi Protected Access 2 (WPA2). INFS 612 [online]. Available from World Wide Web: <URL: http://cs.gmu.edu/~yhwang1/INFS612/Sample_Projects/Fall_06_GPN_6_Final_Report.pdf>

Aruba Networks, Inc. (2011). Wi-Fi Certified Passpoint Architecture for Public Access. [online]. Available from World Wide Web: <URL: http://www.arubanetworks.com/pdf/technology/whitepapers/WP_Passpoint_Wi-Fi.pdf>

Berg Justin (2011). *The IEEE 802.11 Standardization, Its history, Specifications, Implementations, and Future.* Technical Report GMU-TCOM-TR-8. [online]. Available from World Wide Web: <URL: http://telecom.gmu.edu/sites/default/files/publications/Berg_802.11_GMU-TCOM-TR-8.pdf>

Cisco (2000). System Management Configuration Guide, Cisco IOS XE Release 3SE (Catalyst 3850 Switches) [online]. Available from World Wide Web: <URL:http://www.cisco.com/en/US/docs/wireless/controller/5700/software/release/3se/system_management/configuration_guide/b_sm_32se_5700_cg_chapter_01001.pdf>

Disruptive Analysis (2011). Carrier WiFi Opportunities Enabling offload, on load and roaming. [online]. Available from World Wide Web: <URL: http://www.wifiglobalcongress.com/files/disruptive_analysis_ipass_carrier_wifi_2011.pdf>

Ellsberger J. (2013). P-HEVOR - System Requirements and Architecture Version 0.12. NGMN Alliance. [online]. Available from World Wide Web: <URL: http://www.ngmn.org/uploads/media/NGMN_P-HEVOR_System_Requirements_and_Architecture.pdf>

Ericsson (2012). *Achieving carrier-grade Wi-Fi in the 3GPP world.* Review. [online]. Available from World Wide Web: <URL: http://www.ericsson.com/res/thecompany/docs/publications/ericsson_review/2012/er-seamless-wi-fi-roaming.pdf>

Garg, V. (2010). Interworking between WLANs and 3G - Part 1: Interworking objectives & approaches. [online]. Available from World Wide Web: <URL: http://www.eetimes.com/document.asp?doc_id=1278379>

Gautschi, David A. (1981). Specification of patronage models for retail center choice. Journal of Marketing Research 8:2, 162–174.

Gupta v., Rohil M. K. (2012). Information Embedding in IEEE 802.11 Beacon Frame. *Proceedings published by International Journal of Computer Applications® (IJCA.* [online]. Available from World Wide Web: <URL:*http://research.ijcaonline.org/ctngc/number3/ctngc1027.pdf*>

IEEE Std 802.11 (2007). Wireless LAN medium access control (MAC) and physical layer (PHY) specifications.

IEEE Std 802.11a (1999). High-speed Physical Layer in the 5 GHZ Band.

IEEE Std 802.11b (1999). Higher-Speed Physical Layer Extension in the 2.4 GHz Band.

IEEE Std 802.11g (2003). Amendment 4: Further Higher Data Rate Extension in the 2.4 GHz Band.

IEEE Std 802.11n (2009). Amendment 5: Enhancements for Higher Throughput.

IEEE Std 802.11u (2011). Amendment 9: Interworking with External Networks.

Informa (2012). *Understanding today's smartphone user: Demystifying data usage trends on cellular & Wi-Fi networks.* White paper. [online]. Available from World Wide Web: <URL:http://www.informatandm.com/wp-content/uploads/2012/02/Mobidia_final.pdf>

InterDgital (2012). *Cellular-Wi-Fi Integration: A comprehensive analysis of the technology and standardization roadmap.* White paper. [online]. Available from World Wide Web: <URL:http://www.interdigital.com/wp-content/uploads/2012/08/Cellular_WiFi_Integration-White-Paper.pdf>

Kaushik S, Kaushik M (*2012*). An overview of Technical aspect for Wireless Fidelity for Wi-Fi and Wireless Networks. *International Journal of Advances in Electrical and Electronics Engineering.* 1:2, 173- 178.

Lehembre G (2005). Wi-Fi security – WEP, WPA and WPA2. hakin9. [online]. Available from World Wide Web: <URL: http://www.hsc.fr/ressources/articles/hakin9_wifi/hakin9_wifi_EN.pdf>

Liu Y., Li S., Xie ., Xu X. (2012). Security Analysis and Improvements of IEEE802.11u. Hewlett-Packard. [online]. Available from World Wide Web: <URL: http://www.hpl.hp.com/techreports/2012/HPL-2012-243.html>

Microsoft (2008). PEAP Overview. Windows Server. [online]. Available from World Wide Web: <URL:http://technet.microsoft.com/en-us/library/cc754179(v=ws.10).aspxNakhjiri M., Nakhjiri M. (2005). AAA AND NETWORK SECURITY FOR MOBILE ACCESS. John Wiley & Sons Inc. 235.

NICC Standards Limited. (2012). Wi-Fi Roaming Requirements. NICC Document. [online]. Available from World Wide Web: <URL: http://www.niccstandards.org.uk/files/current/ND1650V1.1.1.pdf?type=pdf >

Pushpendra Kr. Verma, Shekhar P, Shekhar J(*2011*). *Competition of Wireless Network Access :Wi-Fi Versus 3G. VSRD International Journal of Computer Science & Information Technology.* 1:2, 44-52.

Rudd S., Torres E., Duncan R. (2011). *Next Generation Hotspot: Maintaining the Profitability of Mobile Data Services.* Transection Network Services. White paper. [online]. Available from World Wide Web: <URL: http://www.tnsi.com/content/images/fromassets/100_1362_240611152707.pdf>

Rukus (2013a). *Hotspot 2.0 Making Wi-Fi as Easy To Use and Secure as Cellular*. White paper. [online]. Available from World Wide Web: <URL:http://www.minedu.fi/kulttuurinen_tietoyhteiskunta>.

Rukus (2013b). It's All About U: Bringing a 3G-like user experience to Wi-Fi authentication and roaming with 802.11u. White paper. [online]. Available from World Wide Web: <URL: http://www2.connectorsystems.co.nz/documents/80211u-WP-101611.pdf>

Sukhija S., Gupta S. (2012). Wireless Network Security Protocols A Comparative Study. International Journal of Emerging Technology and Advanced Engineering [online]. Available from World Wide Web: <URL: http://www.ijetae.com/files/Volume2Issue1/IJETAE_0112_61.pdf>

Telecom Regulatory Authority (2003). WiFi Technology. Technology Tracking Department. [online]. Available from World Wide Web: <URL: http://www.tra.gov.eg/uploads/technical%20material/Wi-Fi%20report.pdf>

Tuladhar S. R. (2007). Inter-Domain Authentication For Seamless Roaming In Heterogeneous Wireless Networks. University Of Pittsburgh. Master Thesis. [online]. Available from World Wide Web: <URL: http://www.computer.org/csdl/proceedings/sutc/2008/3158/00/3158a249-abs.html>

Weston B. (2008). Foundation Network Companion Guide: Deploying 802.1X Authenticated Wireless Access with PEAP-MS-CHAP v2. Microsoft. [online]. Available from World Wide Web: <URL: http://www.microsoft.com/en-us/download/details.aspx?id=8089>

Wi-Fi Alliance [online]. Available from World Wide Web: <URL:http://www.wi-fi.org/knowledge-center/faq/what-does-wi-fi-alliance%C2%AE-do>

Wi-Fi Alliance (2012a). *Wi-Fi CERTIFIED Passpoint™ (Release 1) 6 Deployment Guidelines.* [online]. Available from World Wide Web: <URL:https://wi-fi.org/download.php?file=/sites/default/files/downloads-public/20121010_Passpoint_r1_DP.pdf>

Wi-Fi Alliance (2012b). The State of Wi-Fi Security Wi-Fi CERTIFIED™ WPA2 TM: Delivers Advanced Security to Homes, Enterprises and Mobile Devices. [online]. Available from World Wide Web: <URL: http://www.wi-fi.org/sites/default/files/uploads/files/wp_State_of_Wi-Fi_Security_20120125.pdf>

Wi-Fi Alliance (2012c). Wi-Fi in Healthcare: Security Solutions for Hospital Wi-Fi Networks. White paper. [online]. Available from World Wide Web: <URL: http://www.wi-fi.org/sites/default/files/uploads/files/wp_201202_Wi-Fi_Security_for_Hospital_Networks-Final.pdf>

Wi-Fi Alliance. (2012d). *Frequently Asked Questions on Wi-Fi CERTIFIED Passpoint.* [online]. Available from World Wide Web: <URL: http://www.wi-fi.org/download.php?file=/sites/default/files/downloads-public/20120626_Passpoint_FAQ.pdf>